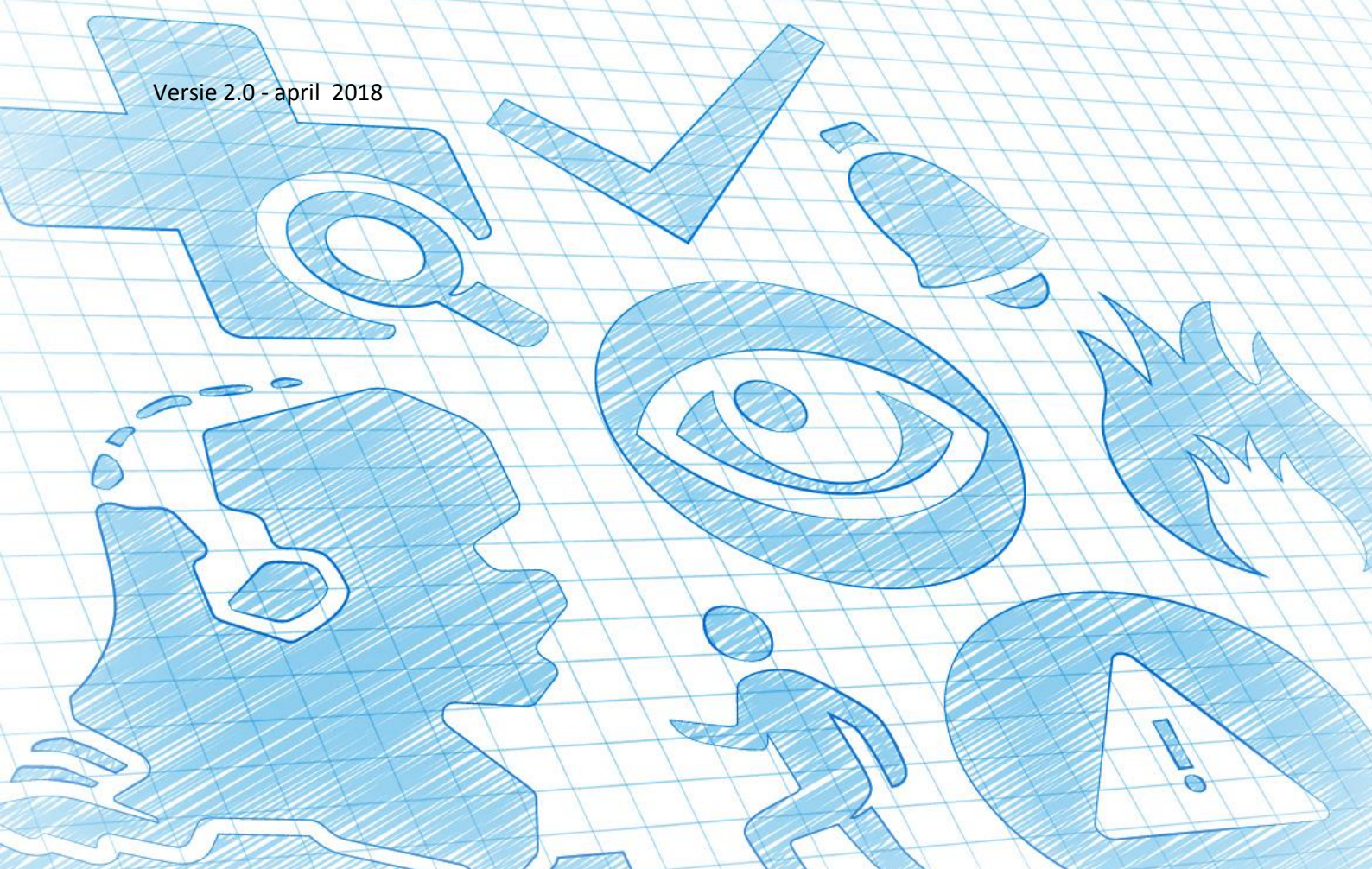
Handreiking Mobiele App Ontwikkeling en Beheer

voor de Rijksoverheid

De Rijksoverheid ontwikkelt steeds meer apps. Maar wat is nu een goede app? Waar moet je rekening mee houden? Welke standaarden zijn er? Deze gezamenlijke uitgave van Belastingdienst, DICTU, SSC-ICT en SSC-I geeft hier antwoord op.

Versie 2.0 - april 2018



Colofon

Afzendgegevens	Shared Service Center ICT (SSC-I) - CTO Office Stavorenweg 3 2803 PT Gouda Postbus 850 2800 AW Gouda www.ssc-i.nl mailto:Ssc-i@dji.minjus.nl		
Auteurs	Belastingdienst (Ministerie van Financiën) DICTU (Ministerie van Economische Zaken en Klimaat), SSC-ICT (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties) SSC-I (Ministerie van Justitie en Veiligheid)		
Versiebeheer	1.0	Maart 2017	Definitieve versie, geaccordeerd in CTO-Raad Rijk
	2.0	April 2018	Concept met de volgende aanpassingen: ▪ Appconfig ▪ AVG ▪ Augmented Reality ▪ Virtual Reality ▪ Unified Endpoint Management (UEM)

Inhoud

Inleiding

Doelstelling

De Handreiking App Ontwikkeling voor de Rijksoverheid draagt bij aan een eenduidige uitstraling, beveiliging en werking van apps van het Rijk. Ze heeft als doel dat organisaties die voor het Rijk apps ontwikkelen gebruik maken van elkaars kennis en ervaring. Deze handreiking omvat een breed scala aan onderwerpen die generiek zijn voor de ontwikkeling en beheer van apps van het Rijk, dit kunnen zowel apps voor de medewerkers van de Rijksoverheid zijn, als apps voor burgers en bedrijven.

Wat is een App?

Een app is meer dan een afkorting van “applicatie”, een app richt zich idealiter op de realisatie van één of enkele functionaliteiten. Dit document richt zich op apps voor mobiele devices (tablets en smart phones en “wearable” devices) en hybride devices (laptops met een los koppelbaar toetsenbord en aanraakscherm). Apps voor niet mobiele devices en onderwerpen gerelateerd aan het “Internet of Things” laten we in deze eerste versie buiten beschouwing omdat de architectuur hiervan volledig afwijkt van die van apps.

Doelgroep

Dit document is bedoeld voor organisaties die apps (laten) ontwikkelen voor het Rijk. Het is zowel technisch als beleidsmatig van aard en gericht op ontwerpers, architecten en ontwikkelaars. Dit document beoogt in de breedte compleet te zijn voor het onderwerp app ontwikkeling voor de Rijksoverheid. Wanneer onderwerpen ergens anders beschreven zijn, wordt daarnaar via hyperlinks verwezen.

Totstandkoming en borging

Deze handreiking is tot stand gekomen in opdracht van de CTO-Raad Rijk aan Belastingdienst, DICTU (Ministerie van Economische Zaken en Klimaat), SSC-ICT (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties) en SSC-I (Ministerie van Justitie en Veiligheid). De inhoud is breed getoetst door partijen binnen de Rijksoverheid die apps ontwikkelen of daartoe opdracht geven. Dit document is opgenomen in de Enterprise Architectuur Rijk (EAR). De verantwoordelijkheid voor het beheer van dit

document ligt bij de portefeuillehouder Enterprise Mobility (EM) voor het Rijk[1], jaarlijks wordt een update ingepland, deze 2018 versie is de tweede update.

[1] Belegd bij SSC-I (Ministerie van Justitie en Veiligheid)

1. Beleid

Het is vanzelfsprekend dat apps van de Rijksoverheid voldoen aan het beleid, standaarden en architectuurkaders van diezelfde Rijksoverheid. Tegelijkertijd moeten apps voldoen aan standaarden die binnen de mobiele wereld gangbaar zijn.

1.1 Beleid en overheidsstandaarden

Tot 2016 was de I-strategie Rijk[2] actief waarmee het kabinet de ICT van de Rijksoverheid wilde verbeteren. Doel van de I-strategie Rijk was o.a. een meer samenhangende infrastructuur en een platform voor tijd-, plaats- en apparaat onafhankelijk werken. Inmiddels (2017) is er een concept van de nieuwe I-strategie; de "Strategische I-agenda voor de rijksdienst[3]".

- Voldoe aan de kaders van de Rijksoverheid.
- Sluit zo veel mogelijk aan op de gangbare publieke (open) standaarden
- Principes als Tijd, Plaats en Apparaat onafhankelijk Werken (TPAW), "De gebruiker staat centraal", loosely coupled architectuur en beveiligingsbewustzijn, zijn leidend.

De Open standaarden van het Forum Standaardisatie[4] en EAR standaarden[5] gelden voor alle aspecten van de voorzieningen van de Rijksoverheid, dus ook voor de dienstverlening via apps. De "Handreiking Mobility 2017 – 2018"[6] van het Enterprise Mobility Rijk (EMR) Expertise Centrum van SSC-I is de handreiking vanuit de Rijksoverheid met betrekking tot de ontwikkeling van een mobiele strategie. Twee technische referentie architecturen voor app ontwikkeling zijn "Referentie architectuur voor mobiele applicaties"[7] van DICTU en "Enterprise mobility referentie architectuur"[8] van de Belastingdienst.

1.2 Publieke standaarden

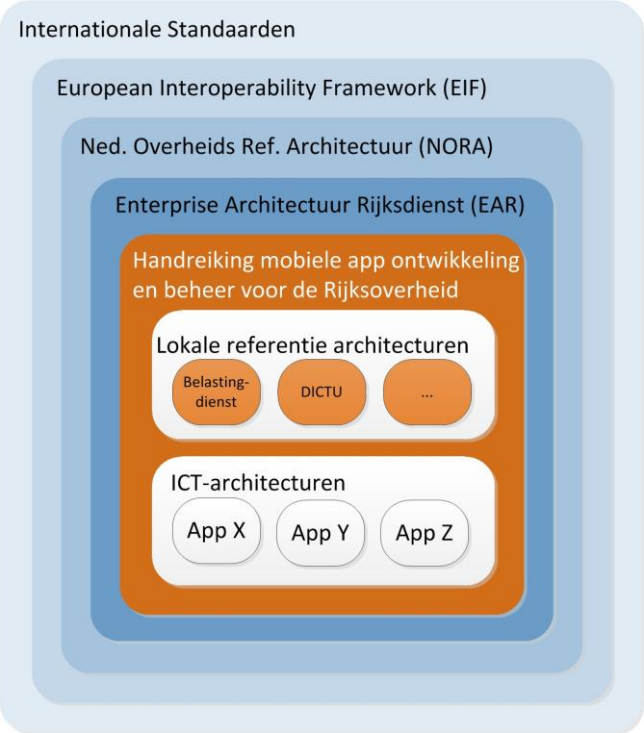
Vanwege het dynamische karakter van de mobiele wereld is het raadzaam om de (open) standaarden van de private sector, zoals leveranciers, te gebruiken. Een voorbeeld hiervan is de Data Driven

[2] https://www.Rijksoverheid.nl/documenten/kamerstukken/2011/11/15/kamerbrief-informatiseringstrategie-rijk
[3] https://www.rijksoverheid.nl/documenten/kamerstukken/2016/12/02/aanbiedingsbrief-bij-de-strategische-i-agenda-rijksdienst
[4] https://www.forumstandaardisatie.nl/lijst-open-standaarden/in_lijst/verplicht-pas-toe-leg-uitlijsten/open-standaarden?lijst=Pas%20toe%20of%20leg%20uit&status%5B%5D=Opgenomen&pagetitle=pastoeof
[5] http://www.earonline.nl/index.php/Overzicht_standaarden
[6] Op te vragen via emr@dji.minjus.nl
[7] Op te vragen via w.j.r.heukers@dictu.nl
[8] Op te vragen via l.versluijs@belastingdienst.nl

Marketing Association (DDMA), de brancheverenigingvoor marketing die adviseert op het gebied van privacy en wetgeving en de DDMA Commissie Mobile opgericht heeft. Eén van hun producten is het document 'Praktische juridische tips mobile'[9]. In dit document wordt de relevante privacywetgeving voor mobile marketing in Nederland omgezet naar de praktijk. Het handboek bevat tevens een handige checklist waarmee is te controleren of een app aan de juridische richtlijnen voldoet.

1.3 Architectuurkaders

Deze Handreiking App Ontwikkeling en Beheer voor de Rijksoverheid kan beschouwd worden als een te realiseren doelarchitectuur van de Enterprise architectuur Rijksdienst (EAR)[10]. De EAR conformeert aan de Nederlandse Overheid Referentie Architectuur (NORA)[11] die weer binnen het (European Interoperability Framework (EIF))[12] valt.



1.4 Principes

Principes zijn een deel van het instrumentarium van iedere architectuur en zijn richtinggevend voor het nemen van besluiten en/of uitgangspunt voor acties. De hieronder genoemde principes voor ontwikkeling van apps zijn afgeleid van de EAR en van best practices uit de mobiele wereld.

Tijd, Plaats en Apparaat onafhankelijk Werken (TPAW). Iedereen kan zijn of haar werkzaamheden onafhankelijk van tijd-, plaats- en apparaat uitvoeren, volgens het EAR principe: "Altijd, overal, ieder apparaat[13]". Dit geldt zowel voor beleidsfuncties als uitvoeringsfuncties. Het TPAW principe beperkt zich niet tot het werken op een vaste werkplek. Men wil overal kunnen werken, dus ook onderweg, op de locatie van een ketenpartner of thuis bij een specifieke doelgroep. Het EAR streefbeeld van TPAW is hier[14] beschreven.

9 https://ddma.nl/juridisch/archief/praktische-juridische-tips-mobile/
10 http://www.earonline.nl/index.php/Welkom_op_de_kennisbank_van_de_Enterprise_Architectuur_Rijksdienst
11 http://www.noraonline.nl/wiki/NORA_online
12 http://ec.europa.eu/isa/documents/isa_annex_ii_eif_en.pdf
13 http://earonline.nl/index.php/Informatiseringsdomein_Werkplekdiensten
14 http://earonline.nl/images/earpub/6/6d/Streefbeeld_TPAW_2015_versie_ICBR_251013_%282%29.pdf

Voldoende veilig. Mobiel werken brengt veiligheidsrisico's met zich mee, bijvoorbeeld doordat bij verlies of diefstal gegevens gemakkelijk "op straat" terecht kunnen komen. Hoe veilig een app moet zijn is afhankelijk van de toepassing van de app en de classificatie van de data in de app. Het hoofdstuk Informatiearchitectuur werkt dit verder uit. De juiste set van beveiligingsmaatregelen wordt bepaald via een risicoanalyse, in het hoofdstuk Beveiliging wordt dit verder uitgewerkt.

Hergebruik van bouwstenen zoals beschreven in het EAR-principe hergebruik bouwstenen[15], bevordert in veel gevallen de efficiency bij ontwikkeling, onderhoud en het beheer. Hergebruik moet echter genuanceerd worden toegepast. Het kan namelijk ook tot kosten-inefficiëntie leiden.

Het **loosely coupled** interacteren (met name met middle tiers en back ends) verhoogt de beheersbaarheid en onderhoudbaarheid van een oplossing. Dit geldt overigens niet alleen voor de mobiele context.

De gebruiker staat centraal. In de mobiele context draait het, nog meer dan bij de ontwikkeling van reguliere software, om de gebruikerservaring. In het hoofdstuk Bedrijfsarchitectuur wordt dit principe uitgewerkt. Bij mobiele apps kan er een trade-off tussen veiligheid en user experience ontstaan.

[15] http://earonline.nl/index.php/Afspraak_-_Gebruik_beschikbare_bouwstenen

2. Bedrijfsarchitectuur

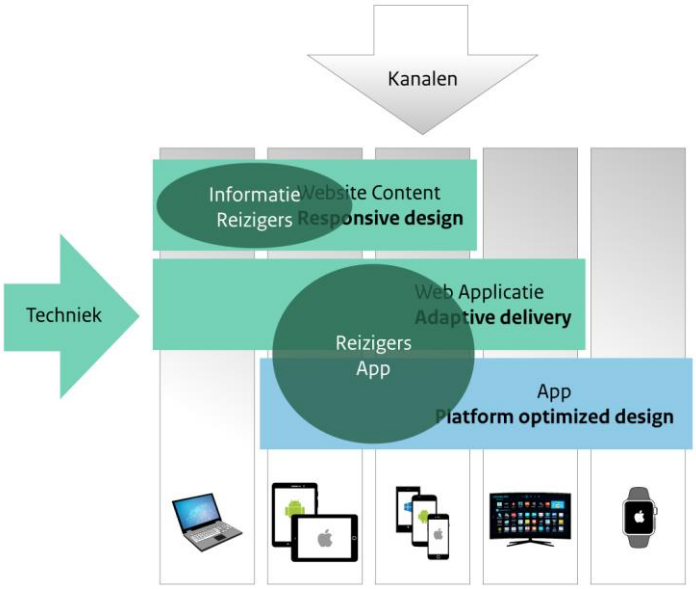
Smartphones en tablets worden vaker en langduriger gebruikt dan computers en laptops. Voor regelmatig terugkerende taken worden vaker apps gebruikt dan websites[16]. Voor de Rijksoverheid is het dus van belang om burgers en bedrijven mobiel te ondersteunen en apps te ontwikkelen.

2.1 Toegevoegde waarde bedrijfsstrategie

Een app moet ten opzichte van de traditionele applicaties of websites toegevoegde waarde leveren die past binnen de bedrijfsstrategie. Het gebruik van een app verhoogt bijvoorbeeld de efficiëntie van de uitvoering van een bedrijfsproces. Apps verhogen de zichtbaarheid van een ministerie of een dienst naar buiten. Op basis van de eigenschappen en de behoeften van de gebruiker bepaalt de organisatie welke diensten mobiel aangeboden worden. De IT-afdeling helpt daarnaast de gebruikers inzicht te krijgen in de nieuwste technieken, wat weer kan leiden tot bijgestelde of nieuwe behoeften.

- Lever via een app toegevoegde waarde aan de bedrijfsstrategie.
- Zorg voor aansluiting van de app op het doel, de doelgroep en de eindgebruiker.
- Laat de app passen in de device-strategie.
- Zorg voor transparantie in het gebruik van informatie door de app.
- Een app is pas een succes als deze veel gebruikt wordt.

Voor mobiele toepassingen is de interactie met gebruikers hoger dan bij traditionele omgevingen. Voor de aanbieder van de app is het eenvoudiger om de gebruiker te bereiken via bijvoorbeeld push-notificaties. Daarnaast biedt een mobiel device toegang tot persoonlijke data als agenda en contacten en beschikt over een scala aan sensoren.



2.2 Aansluiting op de eindgebruiker

Gebruikers zijn gewend aan een groot aanbod van kwalitatief goede apps vanuit de publieke app stores. Het “responsive maken” van websites of applicaties is een

[16] bronnen: o.a. Flurry, Comscore

mogelijke stap om de mobiele gebruiker te bereiken, echter dit levert niet altijd het gewenste resultaat op. Onderzoek bij het aanbieden van mobiele diensten hoe de gebruiker optimaal ondersteund wordt, rekening houdend met factoren als tijdstip, locatie, activiteit, hoeveelheid informatie die getoond wordt op het scherm, hoeveelheid invoer via toetsenbord en mate van interactiviteit. Op basis hiervan kan een keuze gemaakt worden op welke wijze een dienst beschikbaar gemaakt wordt. Deze keuze hoeft niet altijd een eenduidige oplossing te zijn maar kan ook betekenen dat de dienst op meerdere kanalen aangeboden wordt. Bijvoorbeeld niet alleen een app maar ook een website. Een trend is dat berichtendiensten zich ontwikkelen als platform, bijvoorbeeld WeChat. Dit is een nieuw kanaal om gebruikers te bereiken. Er zijn daarbij verschillende manier om het kanaal te benutten. Een organisatie-chat op basis van bijvoorbeeld een chat-bot of, als de berichtendienst het faciliteert, volledige apps geïntegreerd in de berichtendienst.

2.3 Doel en doelgroep

Apps zijn anders dan traditionele applicaties. Apps zijn bedoeld voor het uitvoeren van een bepaalde taak of aan elkaar gerelateerde taken. Voorkomen moet worden dat een app te veel (ongebruikte) functionaliteit in zich heeft en hierdoor complex en moeilijk in gebruik wordt. Tegelijkertijd is het niet gewenst burgers en bedrijven te overspoelen met grote aantallen apps die één specifieke taak uitvoeren. Onderken daarom de doelgroepen voor een app en biedt per doelgroep één app aan met alle relevante functionaliteiten. Bijvoorbeeld een app voor burgers en een app voor bedrijven om te communiceren met de organisatie. Hetzelfde geldt voor interne apps. Niet elke medewerker heeft elke app van de organisatie nodig en ook is het niet wenselijk om één app per organisatie te maken vanwege de afhankelijkheden en autorisaties die gemanaged moeten worden. Voor apps die een primair proces ondersteunen is een goede richtlijn om alle mobiel uit te voeren taken van het betreffende proces in één app te integreren. Dit kan betekenen dat sommige functies in meerdere apps terugkomen. Een voorbeeld hiervan is een functie voor het opvragen van informatie over een voertuig op basis van een kenteken. Deze functie wordt gebruikt bij het proces voor toezicht op betaling van motorrijtuigenbelasting maar ook voor het proces van een deurwaarder voor beslaglegging. In beide gevallen is de informatie ook nodig in het verdere proces en daarom is de functie volledig geïntegreerd.

2.4 Device-strategie

De app houdt rekening met de device-strategie die binnen de organisatie wordt gehanteerd, denk hierbij aan de platformkeuzes, Bring Your Own Device (BYOD)-beleid, autorisatiemogelijkheden en wijze van distributie. Apps voor burgers en bedrijven kennen een diversiteit aan mogelijke platformen (Android, iOS, etc.) en worden gedistribueerd via de publieke app stores. Het platform van de app van de medewerker is over het algemeen bekend omdat de mobiele devices vaak door de organisatie worden uitgegeven. Apps voor rijksambtenaren worden gedistribueerd via een EMM/UEM oplossing

of via enterprise app stores. In het hoofdstuk Beheer en distributie wordt aandacht besteed aan de distributie van apps.

Veel organisaties bieden medewerkers de mogelijkheid om hun privé-device te gebruiken voor zakelijke toepassingen. Vaak zullen naast bedrijfsdevices dus ook privé-devices door een EMM oplossing beheerd worden. Dit is nodig voor toegang tot diensten en beveiliging van informatie. Voor goede BYOD-ondersteuning is het noodzakelijk om een aantal beslissingen te nemen en deze ook helder te communiceren zoals:

1. Welke werkzaamheden voor de organisatie op een privé-device uitgevoerd mogen worden. Is dit beperkt tot E-mail en social apps of is het ook gewenst om primaire processen met gevoelige informatie te ondersteunen op BYOD.
2. Welke platformen en versies (Android, iOS, etc.) voor privé-devices worden ondersteund. Dit zal vaak bepaald worden door de ondersteuning van de EMM leverancier, Wifi bedrijfsnetwerk, E-mail en samenwerking-platform ondersteuning.
3. Privacy-aspecten van het gebruik van eigen apparatuur. Welke informatie van het apparaat of de gebruiker wordt door de organisatie verzameld, verwerkt en opgeslagen. Wat wordt met deze informatie gedaan.

2.5 Transparantie

Mobiele devices bieden veel mogelijkheden en bevatten veel persoonlijke data. De app moet de gebruiker duidelijk maken hoe hiermee wordt omgegaan. De bestaande platformen gaan steeds verder in het beschermen van privacygevoelige data voor hun gebruikers. De nieuwste versies van iOS en Android bijvoorbeeld, zorgen ervoor dat de gebruiker altijd toestemming moet geven voor het gebruik van GPS, camera, toegang tot contacten of de agenda. Hierbij moet de app aangeven wat de reden is voor toegang. Net als websites maken apps ook gebruik van het verzamelen van statistieken. En net als bij websites is het belangrijk dat de gebruiker geïnformeerd wordt en in control is zodat er geen misbruik gemaakt kan worden door commerciële analytics diensten. De verzamelde data kunnen bijvoorbeeld gebruikt worden voor het opbouwen van profielen.

2.6 Succesvolle apps

Tenslotte, het succes van een app ligt ook in het daadwerkelijke gebruik ervan. Zorg dus voor goede communicatie en/of marketing voor de app en het daarvoor benodige budget . Voor publieke apps kunnen hiervoor advertenties en social media worden ingezet. Gebruik voor interne apps een bericht op intranet, interne social media of de klassieke posters ”in de lift”. Monitor het gebruik van de app en breng regelmatig updates met verbeteringen en/of nieuwe functionaliteiten uit . Het vasthouden van het succes vraagt om pro-actief beheer van een app.

3. Informatiearchitectuur

De informatie die in een app komt te staan is van invloed op de ontwikkeling van een app. Mobiele devices bieden meer mogelijkheden in het aanbieden van informatie en er zijn maatregelen nodig om informatie te beschermen.

- Classificeer de informatie die in de app komt te staan.
- De mogelijkheden van een device kunnen bepalen hoe informatie wordt vastgelegd.
- Sla informatie lokaal op met passende maatregelen.
- Combineer informatie uit verschillende bronnen in een app.
- Verrijk de echte wereld met virtuele informatie.

3.1 Classificatie

Afhankelijk van de informatie die een app bevat, moeten bepaalde beveiligingsmaatregelen worden genomen. Door een classificatie van de informatie toe te passen is het mogelijk om standaard maatregelen te definiëren per classificatie. De Algemene verordening gegevensbescherming (AVG) is hierbij het uitgangspunt. De classificering van informatie in apps voor medewerkers kan het beste gebeuren met de bestaande methode binnen de eigen organisatie. Onderstaande figuur bevat een voorbeeld van classificatie niveaus staat in onderstaande figuur.

Niveau	Classificatie informatie publieke apps	Classificatie informatie interne apps
Laag	Publieke informatie	Publieke informatie of Open Data
Midden	Persoonsgegevens	Departementaal Vertrouwelijk
Hoog	Bijzondere persoonsgegevens of financiële gegevens	Departementaal Vertrouwelijk met een hoger dan gemiddeld dreigingsniveau of Staatsgeheim/ Confidentieel

3.2 Vastleggen van informatie

Mobiele devices beschikken over sensoren die mogelijkheden bieden om informatie op een andere manier te vergaren dan alleen de traditionele tekst invoer. Daarnaast bieden platformen een breed

scala aan mogelijkheden om informatie aan de gebruiker te kunnen aanbieden op andere manieren dan in de app zelf.

Invoeren van informatie. Bij het invoeren van informatie is het belangrijk om te bepalen wat de mogelijkheden zijn die standaard geboden worden door de devices. Er zijn twee belangrijke redenen om dit te doen:

- Eenvoudigere invoer, de meeste mobiele devices zijn niet ontworpen om veel tekst in te voeren via een toetsenbord.
- Nauwkeurigheid verhogen, door gebruik te maken van sensoren kun je meer of gedetailleerdere informatie vergaren dan via traditionele tekstinvoer.

Het maken van een foto in plaats van het vragen van een uitgebreide omschrijving biedt niet alleen een gedetailleerde vastlegging maar ook een veel betere gebruikerservaring. Ook kan een foto eventueel aangevuld worden met extra informatie. Een ander voorbeeld is het vastleggen van een locatie via de GPS sensor van een device door middel van coördinaten in plaats van een adres. Veel platformen bieden ook de mogelijkheid om een vertaling te maken van coördinaten naar adresgegevens en omgekeerd om uiteindelijk eenvoudig de gewenste informatie te verkrijgen.

Aangezien het gebruik van sensoren als de camera of GPS ook misbruikt kunnen worden zullen steeds meer platformen het gebruik ervan afschermen. Pas na toestemming van de gebruiker zal de app toegang geven tot de sensoren. Zorg in de app dus voor een heldere uitleg waarom en waarvoor de informatie van de betreffende sensor nodig is, dit wordt ook steeds vaker vereist vanuit de platformleveranciers.

Aanbieden van informatie. Informatie kan in de app zelf worden getoond maar ook zonder de app te openen in de vorm van een notificatie, een widget op een startscherm, via personal assistants (Siri, Google Now, Cortana) of zoekfaciliteiten van het platform. Informatie van buiten de app is eenvoudiger toegankelijk voor de gebruiker en deze kan ook vaak nog een bewerking door de platformleverancier ondergaan. Publieke informatie kan zonder problemen buiten de app worden aangeboden, als het echter over persoonsgegevens of departementaal vertrouwelijke informatie gaat, is het goed om een afweging te maken tussen gebruikerservaring en beveiliging.

3.3 Lokaal opslaan

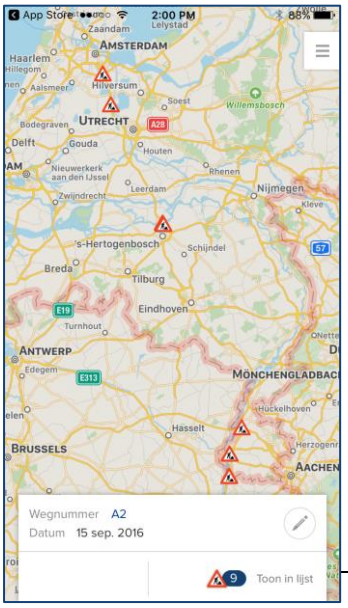
Mobiele devices bieden apps de mogelijkheid om informatie lokaal op het device zelf op te slaan. Dit kan nodig zijn voor een betere gebruikerservaring, voor een lagere belasting van de back end (de systemen waar de app informatie uit haalt) of voor offline gebruik van de app. Aangezien mobiele devices gevoeliger zijn voor verlies of diefstal is het belangrijk om de informatie die lokaal opgeslagen is op een goede, passende manier te beveiligen. Meer informatie over beveiliging van apps is te vinden in het hoofdstuk Beveiliging. Zwaarwegende redenen om lokaal informatie op te slaan zijn:

- **Gebruikerservaring.** Gebruikers zijn gewend dat apps snel reageren. Dit betekent dat informatie die getoond wordt snel beschikbaar moet zijn. Het tijdelijk opslaan (cachen) van gegevens op het device kan ervoor zorgen dat informatie direct beschikbaar is en er niet gewacht hoeft te worden tot de informatie vanuit het datacenter beschikbaar is. Een voorbeeld hiervan zijn E-mail-applicaties waarbij E-mails lokaal opgeslagen worden en deze direct bij opstarten al getoond worden.
- **Belasting van de back end.** Door lokaal data op te slaan kan het aantal vragen naar de back end beperkt worden. Denk hierbij aan lokaal opslaan van statische data die in een app gebruikt wordt zoals lijsten met organisatieonderdelen, landen en regio's.
- **Offline gebruik.** Op sommige locaties is de beschikbaarheid van een verbinding met Internet niet gegarandeerd. Als de app dan ook gebruikt moet kunnen worden dan dient data lokaal opgeslagen te worden. Dit geldt ook voor de ingevoerde data die dan op een later moment verzonden wordt. Een voorbeeld is de Fysiek Toezicht app van de Douane waarmee medewerkers controles uitvoeren.

3.4 Combineren van bronnen

Aangezien apps ook informatie buiten het bedrijfsnetwerk kunnen benaderen is het combineren van informatie van buitenaf met informatie van het interne netwerk een belangrijke mogelijkheid van apps. Door het combineren van informatie kan de dienstverlening verbeterd worden en vaak ook aansluiten op een persoonlijke situatie. Een aantal voorbeelden is hier toegelicht.

Open data. De overheid heeft een ruim aanbod van open data datasets[17]. Deze data combineren met de informatie van de gebruiker of de eigen organisatie kan een verrijking betekenen voor de gebruiker. Een voorbeeld is een medische app die gebruik maakt van open data sets met de actuele luchtkwaliteitsindex en fijnstofconcentratie.



Social Media. Vanuit apps is het mogelijk om snel en eenvoudig te integreren met de mogelijkheden van social media. Via een AMBER Alert app bijvoorbeeld, kan de gebruiker een melding delen op Facebook of Twitter. Een andere toepassing is het gebruik van profielinformatie vanuit social media. Het is hierbij wel belangrijk om rekening te houden met privacy-aspecten en te voorkomen dat geclassificeerde bedrijfsinformatie naar buiten lekt. Een goede voorlichting voor medewerkers is hierbij noodzakelijk.

Kaarten. Vanuit de platformen worden kaartvoorzieningen aangeboden om informatie op een kaart visualiseren. Deze kaarten bieden steeds meer mogelijkheden om additionele informatie te integreren,

[17] https://data.overheid.nl/

bijvoorbeeld verkeersinformatie of locaties van instellingen. Belangrijk bij het gebruik van kaarten is de privacy in de gaten te houden, immers de kaart die opgevraagd wordt bij het platform kan gebruikt worden om een profiel te verrijken. De voorziening Publieke Dienstverlening Op de Kaart (PDOK)[18] van de Nederlandse overheid heeft dit risico niet, het hoofdstuk Geografische functionaliteit gaat hier verder op in.

Agenda, Contacten. Mobiele devices hebben standaard voorzieningen voor E-mail, agenda en contacten en bieden de mogelijkheid om deze te gebruiken in apps. Een voorbeeld hiervan is de BTW Alert app waarbij herinneringen in de agenda van de gebruiker worden geplaatst voor een tijdige aangifte van BTW. Om toegang te krijgen tot de persoonlijke agenda of de contacten moet de gebruiker toestemming geven, zorg dus voor transparantie in de app over het gebruik van deze gegevens.

3.5 Virtual reality, augmented reality en machine learning

Tenslotte, maak gebruik van informatie uit de virtuele wereld om de werkelijkheid verrijken. Doordat mobiele devices steeds meer rekenkracht krijgen en beschikken over een breed scala aan sensoren is er steeds meer mogelijk. Denk aan het tonen van informatie door middel van een mobiel device of een virtual reality (VR) bril om inzicht te geven in een toekomstige situatie of voor trainingstoepassingen. Via augmented reality (AR) wordt de echte wereld getoond in het scherm van een mobiel device en soms levensecht, verrijkt met virtuele informatie. De inzet van machine learning waarbij via modellen en algoritmen artificiële intelligentie toegepast kan worden op de informatie uit de sensoren, biedt mogelijkheden zoals het herkennen van objecten in foto's en het begrijpen van gesproken tekst. Machine learning voor objectherkenning kan in combinatie met AR heel krachtig zijn voor het realtime tonen van informatie in een blik op de echte wereld, biivoorbeeld door op een auto informatie van de eigenaar te projecteren op basis van het kenteken van de auto.

[18] https://www.pdok.nl/

4. Softwarearchitectuur

De softwarearchitectuur voor apps kent in het algemeen een grote diversiteit. Er zijn native apps, web apps en hybride apps en er zijn diverse platformen en versies waarvoor ontwikkeld kan worden. Ook komen specifieke mobiele onderwerpen zoals push-notificaties en geografische functionaliteit aan bod.

4.1 Native, web of hybride

- Native, web of hybride? Kies de type app op basis van de eigenschappen van een technologie en maak deze afweging voor elke app opnieuw.
- Android, iOS of Windows? Kies de platformen op basis van de dekkingsgraad bij de doelgroep.
- Gebruik platform richtlijnen en componenten van de platform leveranciers voor het ontwikkelen van native apps.

Native apps zijn apps gemaakt voor een specifiek platform (Android, iOS, Windows, etc.). De apps zijn op het device geïnstalleerd vanuit de leverancier of netwerkaanbieder. Native apps sluiten wat betreft gebruikerservaring aan op het onderliggende platform, ze bieden een goede beveiliging en ze kunnen beter en dieper gebruik maken van een aantal device-specifieke mogelijkheden, waaronder de sensoren van het mobiele device en de camera. Native apps worden ontwikkeld met daarvoor bedoelde platformtools of met zogenaamde cross-platform tools waardoor code hergebruikt kan worden.

Hybride apps zijn een variant op de native apps waarbij in een browser-container de app op basis van HTML5 en Javascript wordt uitgevoerd. Voordeel hiervan is dat de code hergebruikt kan worden voor alle platformen. Voor toegang tot sommige sensoren moet er per platform code geschreven worden, de toegang tot camera, locatie, microfoon is meestal cross-platform beschikbaar. De gebruikerservaring van hybride apps is afwijkend van de gebruikerservaring van het platform in de zin dat paginaovergangen bijvoorbeeld, door het webgedeelte worden afgehandeld en daardoor minder vloeibaar ogen. Hybride apps bestaan in diverse gradaties van “nativeness”, dit is verder uitgewerkt in de technische referentie architecturen voor app ontwikkeling. In het hoofdstuk Beleid is aangegeven waar deze architecturen beschikbaar zijn.

Web apps (ook wel HTML5 apps genoemd) zijn apps gemaakt met HTML5- en Javascript-technologie die op een server staan en in de browser van het device uitgevoerd worden. De gebruiker kan door een snelkoppeling op het device te maken toegang tot de app verkrijgen. Bij zogenaamde “installable webapps” wordt een icoon op het homescreen van het device geplaatst. Web apps bieden de ontwikkelaar de meeste flexibiliteit. Voor de ontwikkeling zijn vele ondersteunende frameworks beschikbaar. Interessant zijn met name de Javascript frameworks voor verschillende functionaliteiten.

Afwegingen voor app technologie	Native app	Hybride app	Web app
Toekomstvastheid	+	-	+
Communicatie met back end	+	+	++
Update snelheid	=	=	++
Ontwikkelkosten	=	-	+
Beheer/onderhoudbaarheid	=	=	+
Time to market	+	-	+
User experience	++	+	-
Animaties en transities	++	=	=
Kwaliteit ontwikkeltools	+	-	=
Leercurve ontwikkelaar	-	--	=
Sensoren	++	+	=
Native API toegang	++	+	--
Beveiliging	++	+	+
Toegankelijkheid	+	-	=
Offline gebruik	++	=	--
Performance	++	+	-
Beschikbaarheid publieke app stores	++	++	--
Push-notificaties	++	+	=
Vindbaarheid	=	=	+
Interapp communicatie	++	=	-
Toepasbaarheid Augmented reality	+	=	-
Toepasbaarheid Virtual reality	=	-	-

Om de keuze voor een native app, web app of hybride app te maken wordt een scorelijst (zoals de tabel op vorige pagina) gemaakt per technologie, met de eigenschappen inclusief een eventuele weging. In de praktijk geven vaak één of twee eigenschappen de doorslag om voor een technologie te kiezen. Maak de afweging voor elke app opnieuw, gezien de snelheid van ontwikkeling van de technologieën en de leercurve van de eigen organisatie.

Het Forum Standaardisatie heeft een handreiking "Handreiking Web of App?"[19] opgesteld waarin een aantal overwegingen met betrekking tot web apps en native apps op een rij worden gezet. Dit

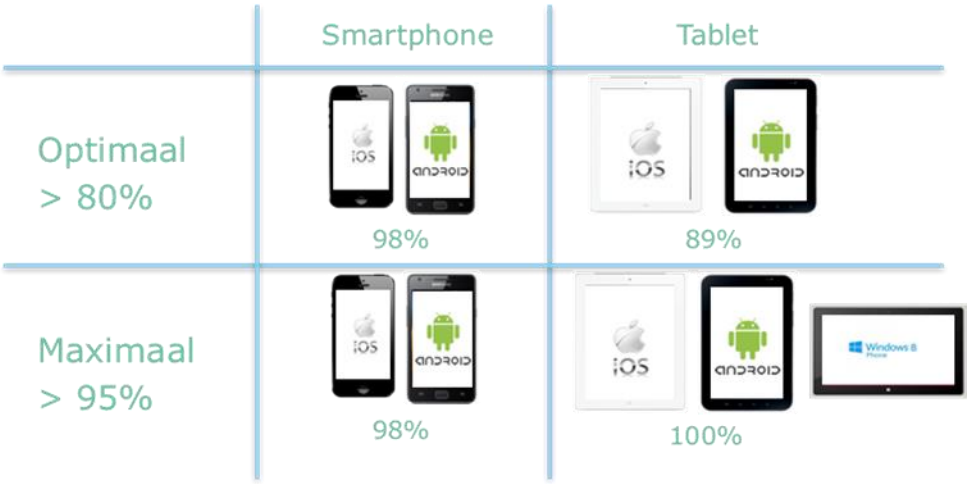
19 https://www.forumstandaardisatie.nl/sites/bfs/files/proceedings/FS%20150923.3A_Handreiking_Web_of_App.pdf

document beoogt door de afweging in technologie en de gedachte de gebruiker centraal te zetten, verder te ondersteunen in de keuze voor een type app.

NB: de hier getoonde kruisjestabel is een opvatting en is gebaseerd op de ervaring van de opstellers van dit document, is getoetst aan marktervaring en het pretendeert niet op ieder moment in de toekomst toepasbaar te zijn.

4.2 Android, iOS of Windows

Apps voor burgers en bedrijven, ook wel **publieke apps** genoemd, kennen een diversiteit aan mogelijke platformen zoals Android, iOS en Windows. In de smartphone context is de rol van Windows inmiddels uitgespeeld. Er zijn andere operating systems, maar dit zijn de meest dominante. De huidige wereldwijde (Q1-2017) marktaandelen voor de platformen voor smartphones zijn wereldwijd: Android 85% en iOS 14,7%, de rest is op dit moment niet relevant meer. (bron IDC[20]). De trend voor tablets is dat Windows wel meespeelt op de tablet markt en daar zelfs weer sterker terugkomt. De cijfers voor Nederland lijken zowel voor smarthones als voor tablets een iets dominantere positie voor iOS weer te geven maar zijn moeilijk eenduidig te krijgen.



Hoe meer platformen ondersteund moeten worden, hoe hoger de kosten van ontwikkeling, testen en beheer. Maak daarom een afweging welke platformen ondersteund moeten worden en realiseer dat ook met mobiele devices niet alle burgers en bedrijven bereikt kunnen worden. Momenteel is het smartphone-bezit in Nederland 85% (bron Telecomnieuwsnet[21]). 68% van de huishoudens heeft een tablet (bron GSMhelpdesk[22]). Bepaal voor apps wat het optimaal bereik moet zijn, bijgaande afbeelding geeft hiervan een voorbeeld. Optimaal betekent dat een groot deel van de gebruikers bereikt wordt tegen redelijke kosten. Maximaal geeft aan de eventueel extra te ondersteunen platform(en) zodat bijna iedereen de app kan gebruiken. Dit betekent wel extra kosten.

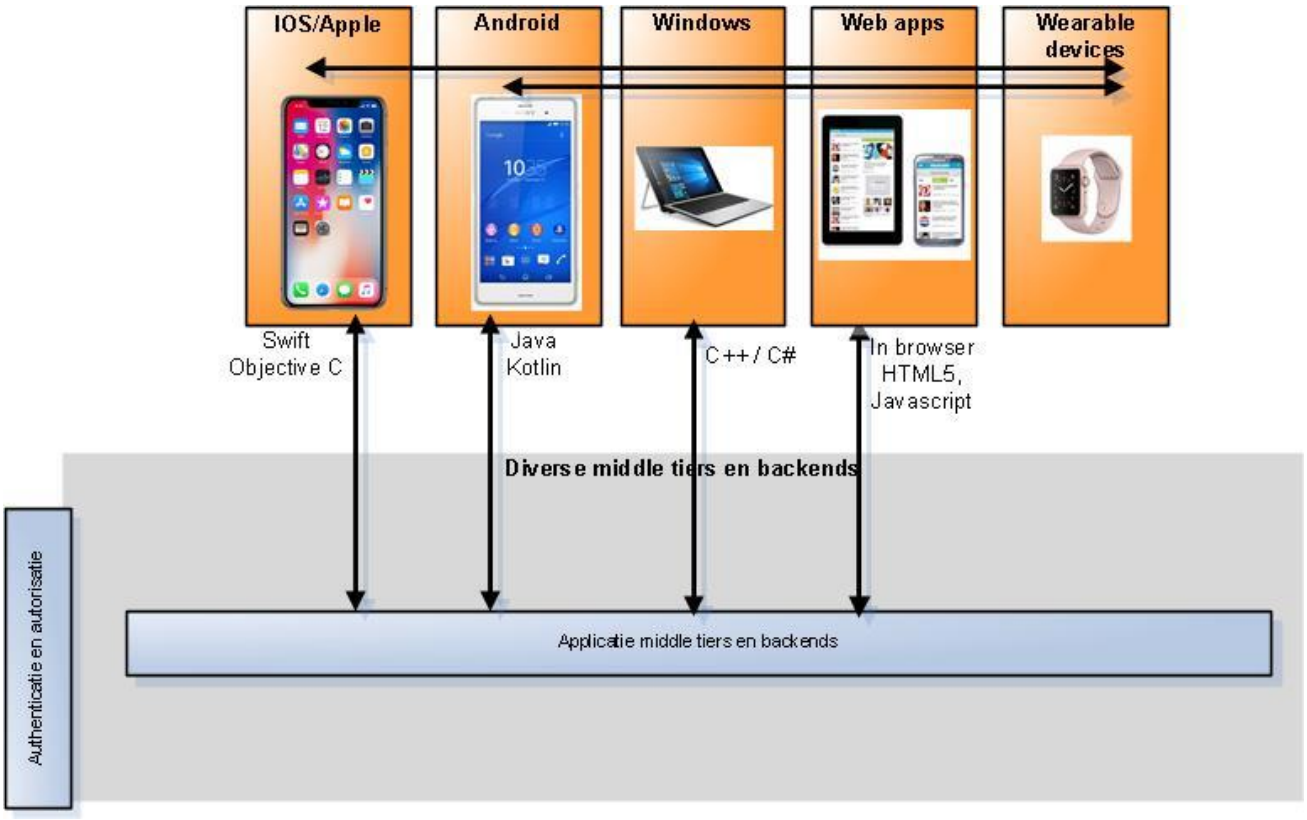
---

20 https://www.idc.com/prodserv/smartphone-os-market-share.jsp
21 https://telecomnieuwsnet.wordpress.com/2016/03/08/onderzoek-smartphonepenetratie-vlakt-in-nederland-af/
22 http://www.gsmhelpdesk.nl/nieuws/12717/68-procent-van-de-nederlandse-huishoudens-bezit-minimaal-een-tablet

Welke platformen ondersteund worden voor apps voor interne medewerkers, ook wel **enterprise apps** genoemd, wordt niet door de markt bepaald maar door de organisatie zelf. Dit hangt samen met het BYOD-beleid, met de EMM\UEM oplossing en soms zelfs met het feit of Wifi-netwerken een OS ondersteunen en E-mail servers er mee overweg kunnen. Default worden meestal iOS en Android ondersteund. De actuele versies van de platformen zijn op te vragen via de volgende hyperlinks: iOS[23], Android[24] en Windows[25].

4.3 Componenten van een app

Een native app bestaat uit een aantal software-componenten. In dit document zijn de mid tier en back end componenten niet weergegeven, in de technische referentie architecturen van DICTU en de Belastingdienst zijn deze wel opgenomen. De invulling van de componenten verschilt per platform. De diverse front ends leggen contact met eventuele back ends, vaak via JSON/REST (verticale pijlen). In het geval van wearable devices is er nu nog vaak een bluetooth-connectie met een smartphone nodig om een app verbonden met het Internet te laten draaien. Bij de nieuwere generaties operating systems van wearables is dit overigens niet meer zo. In de apps zijn uiteraard ook NFC connecties mogelijk.



[23] https://developer.apple.com/support/app-store/
[24] http://developer.android.com/about/dashboards/index.html
[25] http://mobitrends.co.ke/windows-phone-market-share/

De softwarearchitectuur verschilt per type app:

- **Native apps.** Beschrijvingen van de softwarearchitectuur per operating system zijn te vinden via documentatie-sites van de diverse operating systems zoals iOS van Apple[26] en Developers voor Android[27]. Bij het ontwikkelen van native apps is het van belang de leverancier richtlijnen over resource gebruik bij de apps te volgen.
- **Web apps.** De ingezette technologie is vooral HTML5, Javascript frameworks en CSS3. Flexibele grids en media queries zijn technieken die hierin gebruikt worden. “Media queries” is een CSS3 module die het mogelijk maakt om content rendering aan te passen aan condities zoals scherm-resolutie (bijvoorbeeld een smartphone versus een high definition-scherm). Er zijn ook vele Javascript-frameworks om hierin verder te ondersteunen. Bedenk dat veel van de business logica zich hier op de server bevindt.
- **Hybride apps** zijn een combinatie van native en HTML5. Ontwikkeltools als Apache Cordova (voorheen Phonegap) ondersteunen hierin. Een aantal commerciële platformen zijn ook op Cordova gebaseerd.

(Native) Cross-platform oplossingen worden door meerdere tools ondersteund, bijvoorbeeld Mono/Xamarin[28]of Appcellerator[29]. Apps worden ontwikkeld in C# en daarna uitgerold naar meerdere platformen, waarbij de user interface code per platform weer apart gecodeerd moet worden. Een alternatief voor bovenstaande cross-platform oplossingen is om apps voor elk platform separaat (“double native”) te ontwikkelen.

4.4 Push-notificaties

Een push-notificatie is een melding die wordt getoond op een device, meestal vanuit een app. Push-notificaties worden gebruikt om iets te melden aan een gebruiker, ook wanneer de app niet actief is. Deze melding kan de vorm hebben van een tekstbericht, een pictogram in de notificatie ruimte op het scherm (Android) of een markering (badge) bij het app-icoon. Push-notificaties hebben relatief geringe kosten doordat er alleen dataverkeer in rekennig wordt gebracht, in tegenstelling tot bij SMS-berichten.

- Gebruik push-notificaties niet meer dan strikt noodzakelijk. Bij overmaat zal een gebruiker er van af gaan zien.
- Verwerk geen privacygevoelige informatie in een push-notificatie bericht.
- Maak optimaal gebruik van de beschikbare platform mogelijkheden.

Belangrijke aandachtspunten bij het gebruik

[26] https://developer.apple.com/
[27] https://developer.android.com/index.html
[28] www.xamarin.com
[29] http://www.appcelerator.com/

van push-notificaties zijn:

- Push-notificaties zijn app specifiek. Alleen als de ontvanger de betreffende app heeft geïnstalleerd kunnen de berichten worden ontvangen. De inhoud van een bericht moet altijd gerelateerd zijn aan de functionaliteit van de app.
- Ga voorzichtig om met het versturen van push-notificaties, omdat een overvloed aan berichten vaak als hinderlijk wordt ervaren en ertoe kan leiden dat de gebruiker de app weer verwijdert of de push-notificatie functie uitschakelt.
- Push-notificaties lopen voor het grootste gedeelte over publieke infrastructuur van de aanbieders van de platformen (Apple, Google en Microsoft). Hoewel deze verkeersstroom encrypted is, impliceert dit dat er een afweging gemaakt moet worden of en zo ja welke privacygevoelige informatie er in een dergelijk notificatie verstuurd kan worden.
- Push-notificaties kunnen zichtbaar zijn op het toegangsscherm van een device (zonder dat er toegang tot het apparaat is gekregen via bijvoorbeeld een pincode). Dit kan afgeschermd worden door een gebruikersinstelling. Echter bij de inhoud van te versturen berichten is deze ongeautoriseerde zichtbaarheid een gegeven om rekening mee te houden.
- Er is geen directe verbinding met het device van de gebruiker waardoor de afleversnelheid van een bericht niet is gegarandeerd.
- Vraag bij in het in gebruik nemen van een app altijd toestemming voor het mogen versturen van notificaties waarbij een goede onderbouwing voor dit gebruik wordt gegeven. Stel de gebruiker eenvoudig in staat deze beslissing te herzien. Alhoewel de daadwerkelijke toestemmingsverlening ook een onderdeel is van het onderliggende operating system, is het raadzaam vanuit de app een goede onderbouwing voor het gebruik van de pushberichten te geven om een gebruiker hier een verantwoorde keuze te laten maken.
- Geef een gebruiker waar mogelijk invloed op de frequentie en detaillering van de push-notificaties via een instelling in de app, zodat de gebruiker in controle is over o.a. de eigen privacy.

Bij de start van een app-ontwikkeltraject dient een zorgvuldige afweging met betrekking tot de te gebruiken push-notificatie-dienst te worden gemaakt. De drie grote platform leveranciers (Apple, Google en Microsoft) hebben ieder hun specifieke wijze en infrastructuur om meldingen naar hun platformen en devices te sturen. Conceptueel werken deze oplossingen op dezelfde wijze. Ook zijn er hybride oplossingen beschikbaar die in staat zijn om vanuit een enkel punt berichten naar de diverse platformen te kunnen verwerken. Bij deze laatste hybride oplossingen is er een keus tussen gratis en betaalde diensten. Houd hierbij ook rekening met de privacy-aspecten van push-notificaties. Zowel de verkeersgegevens (wie zijn de ontvangers) als de inhoud kan relevant zijn bij deze keuze. Wat zijn bijvoorbeeld het businessmodel en gebruiksvoorwaarden van een aanbieder? Wat kan en mag deze met de gegevens doen en is dit een risico?

Voor de werking en details van de verschillende push-services wordt verwezen naar de ontwikkelaarspagina's van de verschillende aanbieders: Apple[30], Android[31] en Microsoft[32].

4.5 Geografische functionaliteit

Mobiele devices bieden, door hun sensoren, geografisch (of locatie) gebaseerde functionaliteit waar apps gebruik van kunnen maken.

Locatie-gebaseerde functionaliteit is in te delen in de volgende categorieën:

- **(Kaart-)visualisatie.** Een kaart in een app met relevante ruimtelijke objecten zoals 'points of interest', percelen, gebouwen, wegen en waterlopen. Het kan een tweedimensionale kaart zijn of een 3D 'scene view', een vorm hiervan is een Augmented Reality view van de omgeving.
- **Ruimtelijke analyse.** Analyse van ruimtelijke informatie tot afgeleide informatie. Voorbeelden van ruimtelijke analyse zijn reisafstand op basis van huidige locatie en afgeleide omgevingswaarden zoals milieuwaarden per locatie (fijnstof, stikstof) of de kans op bepaalde gebeurtenissen (aardbeving, overstroming).
- **Inwinnen en vastleggen van ruimtelijke gegevens.** Registratie van ruimtelijke objecten zoals locaties van objecten (leidingen in de grond, percelen, gebouwen) en registratie van inspecties zoals "de losse stoeptegel" of te vernieuwen wegdelen, of geplande ruimtelijke zaken zoals locaties van braderie-kramen. Hierbij kan ook locatie gebonden beeldinformatie worden ingewonnen (foto's of video's).
- **Location tracking.** Het tracken van de locatie van een device om functies te realiseren als:
  - **Navigatie.** Het uitvoeren van een netwerkanalyse voor optimale / gewenste routering van transport.
  - **Geofencing**. Een melding bij het naderen of bereiken van een bepaald gebied of bepaalde afstand van een ruimtelijk object of persoon. Beacons (Wikipedia[33]) kunnen een ondersteunende rol spelen bij geofencing.

- Betrek geografische expertise indien nodig.
- Sluit aan op de gangbare Geostandaarden.
- Gebruik overheidsbrede bouwstenen van PDOK.

Het gebruik van geografisch gebaseerde functies is nauw verweven met het domein van Geografische Informatiesystemen (GIS). Dit is een specifiek kennisgebied binnen de ICT waarbij verschillende

[30] https://developer.apple.com/app-store/review/guidelines/#push-notifications
[31] http://developer.android.com/design/patterns/notifications.html
[32] https://azure.microsoft.com/en-us/documentation/articles/notification-hubs-overview/

[33] https://en.wikipedia.org/wiki/Bluetooth_low_energy_beacon

aspecten meespelen zoals specifieke standaarden, verschillende soorten geodata, overheidsbrede bouwblokken, coördinatenstelsels, kaartprojecties en nauwkeurigheid. Voor meer informatie zie de NORA-pagina over Geo[34].

In het GIS-domein zijn diverse leveranciers[35] actief. Daarnaast zijn er verschillende volwassen Open Source producten zoals web mapping libraries (OpenLayers, Leaflet), GIS-servers (Geoserver, Deegree) en tools voor bewerking en analyse (QGIS, MapWindow). De Publieke Dienstverlening Op de Kaart (PDOK)[36] is een overheidsbrede voorziening waarin allerhande geografische informatie beschikbaar is:

- Basiskaarten/achtergrondkaarten.
- Gegevens uit diverse Basisregistraties: adressen en gebouwen, topografie, kadaster.
- Hoge resolutie luchtfoto's.
- Allerlei open data sets, zoals natuurgebieden, bestemmingsplannen, etc.

De toegang is hetzij openbaar, hetzij beveiligd via de PDOK toegangslaag.

Verder is er binnen diverse overheden vaak een voorziening ingericht voor toegang tot de diverse Basisregistraties. Daarmee kunnen gegevens zoals kadastrale percelen, NHR-bedrijfsgegevens en adressen en gebouwen worden gebruikt in GIS-enabled apps op mobiele devices. Deze gegevenssets zijn nog rijker dan die van PDOK en kunnen in onderlinge samenhang worden bevraagd.

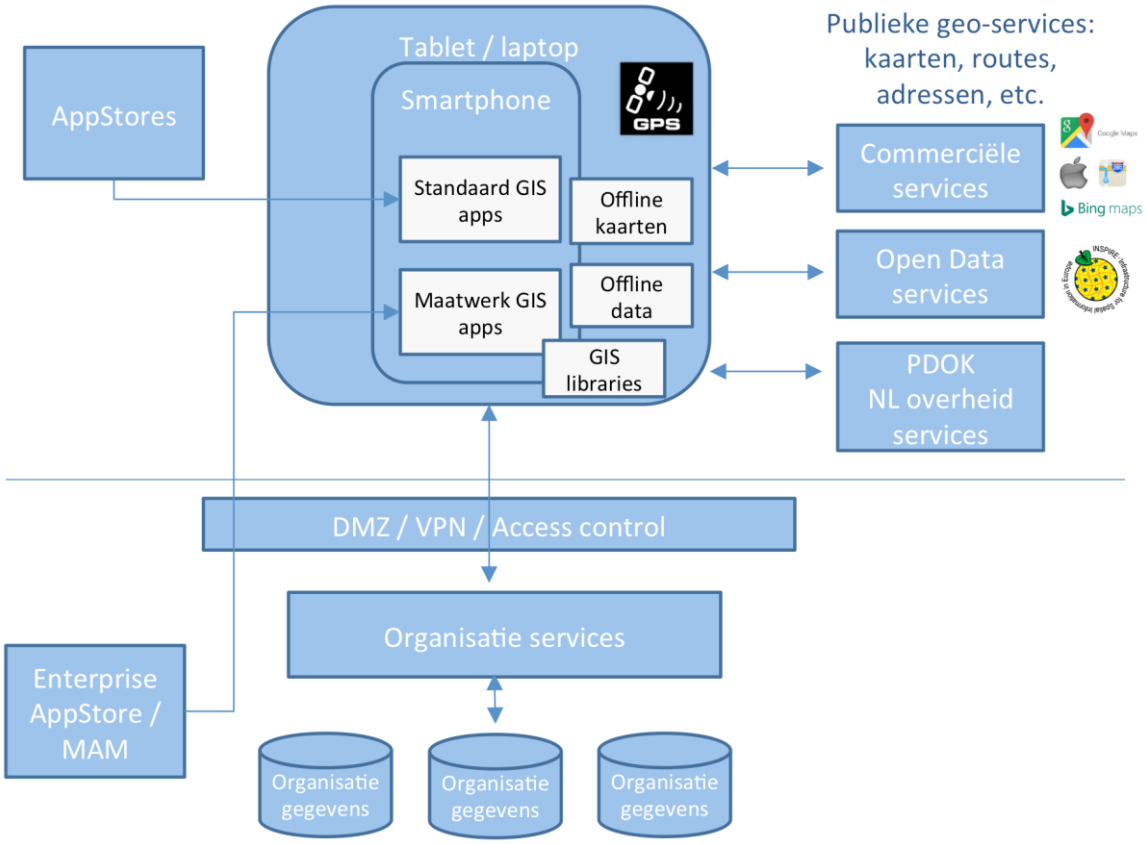
Voor ieder van bovengenoemde functies (Kaartvisualisatie, Ruimtelijke Analyse, Inwinnen gegevens, Location/Device tracking) kunnen tools worden ingezet. Het voert te ver om hier alle tools uitgebreid te beschrijven. In de volgende figuur wordt de algemene architectuur van apps met geografische functies weergegeven:

- Er zijn standaard apps beschikbaar in de app stores die gebruik kunnen maken van geografisch gebaseerde functies. Voorbeelden: Google/Apple Maps, en andere, specifiekere mapping apps. Houd de privacy hierbij in de gaten, het feit dat de locatie van iemand door Apple, Google, Microsoft kan worden vastgelegd.
- Er kunnen maatwerk-apps ontwikkeld worden binnen een organisatie, die gebruik kunnen maken van de native OS geo functies, maar ook van geo-libraries.
- Apps kunnen offline kaarten opslaan op het device van een beperkt (werk)gebied.
- Apps kunnen geo-gegevens lokaal opslaan en synchroniseren met back end services.
- Apps kunnen gebruik maken van diverse publieke services: commerciële kaart-functies, open data services, en services van PDOK.nl.

[34] http://www.noraonline.nl/wiki/Geo

[35] https://en.wikipedia.org/wiki/List_of_geographic_information_systems_software#Companies_with_high_market_share

[36] https://www.pdok.nl/



Locatie en Geofencing. Geofencing is het virtueel afbakenen van een geografisch gebied door middel van GPS. De meeste toepassingen vind je terug op mobiele apparaten als tablets en smartphones. Geofencing wordt daarop mogelijk door gebruik te maken van de locatiediensten die tegenwoordig op ieder mobiel device geïntegreerd worden[37]. In het algemeen zal geofencing de volgende stappen vergen:

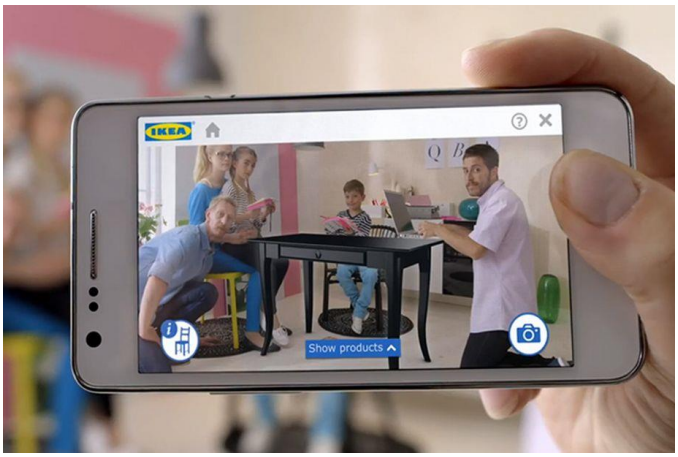
- Bepalen van geofence(s) oftwel 'interessegebieden': geofences ophalen van een service, en/of bepalen op basis van huidige locatie.
- Afhandelen van geofencing events: als het device een geofence binnenkomt of verlaat, of meer of minder dan een bepaalde tijd in een geofence verblijft. Op dat moment kan de gebruiker een notificatie krijgen, en/of er kan een remote service aangeroepen worden om het geofencing event te melden.

Geofencing kan ook bereikt worden door geofences in een back end systeem te registreren en devices periodiek hun locatie te laten sturen naar de back end die vervolgens de geofencing events afhandelt. Dit vereist wel connectiviteit tussen devices en back end. Let bij vastleggen en volgen van locatie en bij geofencing goed op privacy-aspecten.

[37] Bron: http://computerworld.nl/security/78231-wat-is-geofencing

4.6 Augmented Reality

Bij Augmented Reality (AR) in de mobiele context, wordt evenals bij Virtual Reality, onderscheid gemaakt tussen augmented reality op headsets en augmented reality op apparaten als smartphones en tablets (mobile AR). Deze handreiking focust nu alleen op mobile AR. De toegevoegde waarde van AR in apps is dat digitale gegevens kunnen worden toegevoegd aan een door de camera getoond beeld.



In de API's van Google en Apple zijn mogelijkheden gekomen om AR functionaliteit aan apps toe te voegen. Inmiddels zijn er in de appstores de nodige AR apps beschikbaar. Apple maakt vanaf iOS11 via de AR-kit library[38] (een framework voor app-ontwikkelaars) vele nieuwe toepassingen mogelijk op het gebied van AR, die gemakkelijk te integreren zijn in iOS apps. Android realiseert dit via het Tango project[39] en ARCore[40]. Op moment van schrijven is Apple verder op het gebied van AR of in ieder geval er wat eerder bij. ARCore is de vervanging van Tango (en de reactie van Google op ARKit). ARCore is nog in de developer preview, maar is functioneel wel vergelijkbaar met Tango. Apple is toegankelijker op het gebied van AR dan Android omdat de AR-kit werkt op alle nieuwe Apple toestellen met iOS11 en Tango en de ARCore preview alleen nog op selecte modellen. Naast de AR-kit van Apple en Tango van Android zijn er nog vele andere frameworks om AR op mobiel te realiseren.

Apple's AR-tool werkt ook samen met Metal, SceneKit, Spritekit en third-party tools zoals Unity en Unreal Engine. Met name Scenekit en Spritekit zijn geschikt voor het creëren van 3D resp 2D objecten, die in de AR app toegevoegd kunnen worden. Voor de user experience van AR, zie het hoofdstuk User Experience.

Test altijd in hoeverre de AR app goed werkt voor de verschillende versies van het betreffende Operating System.

4.7 Virtual reality

Virtual reality is een kunstmatige, volledig computer-gegenereerde simulatie omgeving of situatie. Hiervoor zijn doorgaans head-mounted displays nodig (HMD's). Hierbij wordt je volledig ondergedompeld in een virtuele 3D wereld (immersive experience). Er zijn flink wat ontwikkelingen in de VR wereld gaande. Denk hierbij aan 360 graden video (Youtube Facebook 360, Hollywoord VR, VR

[38] https://developer.apple.com/arkit/
[39] https://developers.google.com/tango/
[40] https://developers.google.com/ar/

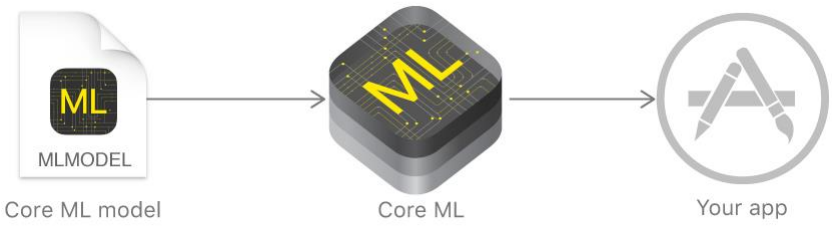
gaming, Life sports , Social VR, VR chat en VR in de verkoopwereld van auto's en huizen, etc). Onderscheid moet worden gemaakt tussen VR headsets die zelfstandig werken (zonder smartphone er in gestoken) zoals de Oculus Rift, de HTC Vive en de Sony Playstation VR en mobiele VR headsets waar de smartphone ingestoken wordt, zoals de Samsung Gear VR, de Google Daydream View en de Merge VR Goggles. Deze handreiking beperkt zich tot de mobiele VR headset applicaties.
Complexe VR toepassing kunnen door programmeurs geschreven worden in de Virtual Reality Modelling Language (VRML) waarin objecten worden gedefinieerd. Alternatief is een ontwikkeltool zoals Unity3D waarin VR applicaties gemaakt kunnen worden, geschreven meestal in C#. De in Unity geschreven code kan geconverteerd worden naar IPA files (iPhones) of APK files (Android) en kunnen verder op de standaard manieren gedeployed worden naar de smartphones.

4.8 Machine learning

Machine learning (ML)wordt steeds meer naar het mobiele device gebracht. Modellen die buiten mobiele devices gegenereerd zijn kunnen in de app gebruikt worden. Met gebruikmaking van de modellen in de apps kunnen er functionaliteiten als realtime beeld herkenning, objectherkenning, sentiment analyse, handschrift herkenning, emotie-detectie, gezichtsherkenning, spreker identificatie en vele andere zaken gerealiseerd worden.

Apple heeft hiervoor o.a. de ML-Kit uitgebracht die naadloos in iOS11 is opgenomen. Android heeft meerdere manieren om ML te integreren in apps. Android beschikt over de Tensorflow Lite libraries en de Android Neural Networks api. Hoe deze te gebruiken zijn, valt buiten de scope van deze handreiking.

Ook heeft Apple een nieuwe machine learning framework API voor developers geintroduceerd, Core ML. Met Core ML zijn machine learning modellen te maken die in een app te integreren zijn. Er zijn vele soorten modellen beschikbaar. Core ML is gebouwd op lowlevel componenten als Metal en Accelerate en hiermee kun je getrainde machine learning modellen in een Swift app integreren.



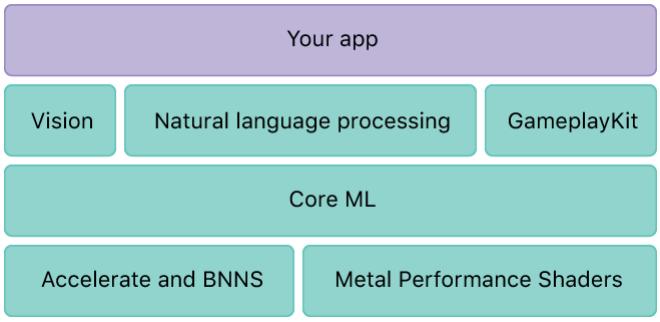
Bron developer.apple.com

Deze modellen zijn offline getraind door specifieke tools. Bekende training tools voor deep learning zijn o.a. Caffe, Keras en TensorFlow. Onderliggend bij deze tools kunnen neurale netwerken betrokken zijn. Een getraind model is het resultaat van het toepassen van een machine learning algoritme op een set van training data. Het model doet voorspellingen gebaseerd op nieuwe input data. De modellen

worden in de eerste stap geconverteerd naar een CoreML model. Daarna zijn ze te gebruiken door de app.

Van belang is om te weten dat het ML Framework zelf bepaalt of het bepaalde reken- intensieve taken op de GPU realiseert, dan wel memory-intensieve taken naar de CPU. Dat hoeft de developer niet zelf te programmeren.

CoreML ondersteunt o.a. Vision (object herkenning) middels het Vision framework en NLP (natural language processing) middels de NLP-API's. Zowel het Vision-framework als de NLP-API's zijn vanuit Swift apps aan te roepen.



Bron: developer.apple.com

5. Integratiearchitectuur

Een app is vaak onderdeel van een mobiele dienst, waarbij de app communiceert met een achterliggende informatiesysteem (back end), dit valt onder het onderwerp Integratiearchitectuur.

5.1 Standaard producten

Mobiele devices verbinden via het Internet met een back end systeem in het eigen datacenter of in de Cloud. Om dit veilig en zo beheersbaar mogelijk te maken is het aan te raden een standaardproduct of combinatie van producten te gebruiken. Het voordeel hiervan is dat de beveiliging gecontroleerd is en up-to-date gehouden wordt door een vertrouwde leverancier. Er zijn drie soorten standaardproducten mogelijk om de communicatie tussen app en back end mogelijk te maken.

- Gebruik standaard producten voor integratie tussen apps en back end systemen.
- Ontwerp diensten en apps voor de toekomst.
- Valideer de schaalbaarheid en beschikbaarheid van back end systemen.
- Gebruik moderne protocollen voor de communicatie.

- **Enterprise Mobility Management (EMM) en zijn opvolger Unified Endpoint Management (UEM)** [41] is een verzameling producten die het beheren van devices en enterprise apps mogelijk maakt. Een onderdeel van het beheren van apps is de mogelijkheid om apps via een Virtual Private Network (VPN) toegang te geven tot het netwerk. Dit kan via de standaard platformmogelijkheden van iOS en Android. Een aantal producten biedt ook een eigen connectiemogelijkheid vanuit een beveiligde container. Deze laatste biedt voordelen, maar bedenk ook dat er dan een extra afhankelijkheid is om rekening mee te houden bij updates. Platform leveranciers raden het gebruik van containers niet aan omdat zij uitgaan van beveiliging op device-niveau.
- Een **Application Programming Interfaces (API) Gateway** is een product dat diensten door API's beschikbaar stelt voor de buitenwereld. Dit hoeft niet exclusief voor apps te zijn. Met een API Gateway is het mogelijk om de beveiliging en de toegang te regelen en het verkeer te controleren alvorens het door te sturen naar de back end. Een API Gateway kan ingezet worden voor enterprise apps en publieke apps. Enterprise service bus (ESB) producten kunnen hiervoor ook ingezet worden maar zorg dan wel voor de juiste

[41] EMM\UEM is beschreven in het hoofdstuk Beheer en distributie

zonering zoals in de Nora beschreven. In het hoofdstuk Infrastructuur- architectuur wordt dit model toegelicht.

- Een **Mobile Enterprise Application Platform (MEAP)** is een productsuite van een leverancier waarin een geïntegreerde ontwikkel- en operationele omgeving aangeboden wordt. Onderdeel hiervan is communicatie vanuit de app naar de back end en de beveiliging daarvan. Naast communicatie faciliteert de MEAP vaak aggregatie en transformatie van gegevens om deze te optimaliseren voor een mobiel device. Bij een MEAP is het wel goed om de volgende aspecten mee te nemen:
    - Extra afhankelijkheid bij updates van platformen.
    - Kosten in relatie tot de onderdelen uit de suite die daadwerkelijk gebruikt gaan worden.
    - Voor de verschillende onderdelen uit de suite kunnen betere gespecialiseerde producten beschikbaar zijn die meer mogelijkheden bieden.

5.2 Update strategie

De gebruiker heeft de controle over het updaten van apps. Dit betekent dat in de eerste versie van een app al duidelijk moet zijn hoe met updates omgegaan wordt. Een belangrijke strategie is om de diensten waar een app gebruik van maakt te voorzien van versies. Hierdoor hoeven niet alle gebruikers de app te updaten om gebruik te kunnen blijven maken van een dienst. Als verschillende versies van een dienst niet wenselijk zijn of er moet toch één versie van een dienst uitgezet worden dan is het belangrijk om dit kenbaar te kunnen maken in de app. Zorg er dus voor dat de app altijd een life cycle management-controle uitvoert. In de praktijk zijn er de volgende mogelijkheden:

- De app is up-to-date, de gebruiker kan de app gewoon gebruiken.
- Het advies is om over te gaan op een nieuwe versie, de gebruiker kan de app nog blijven gebruiken.
- Er is een verplichting om direct over te gaan op een nieuwe versie, de app is niet meer te gebruiken.
- Er is een verplichting om het operating system te updaten vanwege beveiliging, de app is niet meer te gebruiken.
- De app is tijdelijk niet bruikbaar vanwege een productie probleem, de app is niet te gebruiken.
- De app is end-of-life en wordt niet meer ondersteund.

Bij apps voor medewerkers is het wenselijk om een EMM\UEM-oplossing te gebruiken om de nieuwste versie pro-actief te pushen naar de gebruiker en onveilige operating system-versies te weigeren.

5.3 Schaalbaarheid en beschikbaarheid

Apps maken vaak gebruik van de data uit back end systemen. Deze systemen zullen niet altijd 24x7 beschikbaar zijn voor de app terwijl gebruikers dat wel verwachten. Indien een back end systeem niet 24x7 beschikbaar is, zijn er de volgende mogelijkheden:

- Zorg dat de app alleen tijdens de 'openingsuren' van het back end systeem kan werken.
- Update het back end systeem voor 24x7 beschikbaarheid.
- Cache informatie in een tussenliggend systeem of in de app zelf zodat de gebruiker niets merkt van het feit dat het back end systeem niet beschikbaar is. Bij caching in de app heeft deze variant als voordeel dat er ook goed omgegaan kan worden met situaties waar geen verbinding naar het Internet is.

Zorg dat de back end systemen voldoende schalen om eventuele extra belasting vanuit de app aan te kunnen. Een voorbeeld is de app Telebankieren waarbij het aantal uitvragingen van het banksaldo vele malen hoger is in de app dan via het web. De gebruiker kan namelijk veel sneller (eenvoudig inloggen) en vaker (altijd mobiel bij de hand) het saldo opvragen. Banken hebben hiervoor hun back end systemen moeten opschalen.

5.4 Communicatieprotocollen

Communicatie met mobiele devices gaat over een netwerk dat niet altijd snel en betrouwbaar qua beschikbaarheid is. Het is daarom belangrijk om ervoor te zorgen dat de protocol- en formaat-overhead beperkt blijft en dat berichten klein blijven. Het meest gebruikte protocol is JSON/REST en dit wordt goed door alle platformen ondersteund. Naast tekst kunnen ook foto's of video's onderdeel uitmaken van het bericht. Het is raadzaam om in dat geval het bericht op te delen en de relatief grote foto- en videobestanden apart te versturen in een geoptimaliseerd formaat. Uiteraard dient de communicatie altijd over een beveiligde verbinding te lopen, denk aan HTTPS met certificate pinning of een VPN.

5.5 AppConfig

Mobiele operating systemen zoals iOS en Android bieden standaard mogelijkheden voor beheerders om data en apps beter te beveiligen door inzet van een EMM\UEM oplossing. Om apps optimaal configureerbaar te maken is door een aantal EMM\UEM leveranciers het AppConfig initiatief gestart. Voor verdere informatie zie AppConfig[42]. De meeste van deze voorzieningen vragen geen of een kleine ontwikkelinspanning (bijvoorbeeld het gebruik van een VPN of configuratie parameters). Sommige voorzieningen kunnen zelfs ontwikkelwerk besparen omdat de functionaliteit standaard beschikbaar is, bijvoorbeeld het verbieden van schermafdrukken of copy/paste. Door de handleiding

[42] https://www.appconfig.org/

van AppConfig te volgen zijn apps ook eenvoudig herbruikbaar door andere organisaties. Een voorbeeld van een AppConfig compatible app is iBabs Pro.

6. User experience

User experience gaat over de ervaring die iemand heeft bij het gebruik van een product. Bij apps van en voor de Rijksoverheid moet voorop staan dat de gebruiker op een positieve wijze ervaart dat hij of zij met de Rijksoverheid te maken heeft. Dit begint met de herkenbaarheid van de Rijksoverheid als afzender van de app. Daarnaast gaat het om het uiterlijk en de werking van de app. Dit document kan geen totaalbeeld geven van wat het vakgebied user experience inhoudt, hiervoor zijn goede publicaties beschikbaar (bijvoorbeeld "Mobile Usability" van Nielsen/Budiu[43]).

- Pas de Rijkshuisstijl toe binnen de platform specifieke richtlijnen.
- Focus in het ontwerp op de primaire doelgroep en houd rekening met specifieke doelgroepen.
- Een app is specifiek en taak gericht. Maak er geen portaal van.
- Gebruik alleen woorden in de icoon van de app als ze onderdeel zijn van het logo. Voorzie het launch screen van het Rijksoverheid-logo.

6.1 Rijkshuisstijl en platform specifieke richtlijnen

Apps voor de Rijksoverheid moeten wat betreft User experience voldoen aan twee typen standaarden, de Rijkshuisstijl voor apps[44] en de technische standaarden die door de leveranciers van de platformen (Apple, Android en Windows) worden uitgegeven. Daarnaast zijn er algemene richtlijnen voor het ontwerpen van een app, bijvoorbeeld de standaarden[45] vanuit het W3C, een organisatie die als doel heeft de interoperabiliteit van het World Wide Web te verzekeren.

De Rijkshuisstijl geeft standaarden voor kleurgebruik (ook online kleuren), het gebruik van logo's, pictogrammen, lettertypen en vlakverdeling. Voor het gebruik van het Rijksoverheidslogo (het "lint") bijvoorbeeld is het van belang vanuit welke Rijksoverheidsonderdeel of externe partij de app wordt uitgegeven (de afzender). De Rijkshuisstijl is van oorsprong opgezet voor traditionele media en wordt steeds meer geschikt gemaakt voor digitale communicatie. In sommige gevallen kan het toepassen van de Rijkshuisstijl conflicten opleveren met het conformeren aan leveranciers standaarden. Een aantal ontwikkelorganisaties binnen de Rijksoverheid hebben daarom eigen richtlijnen gemaakt, de

[43] Nielsen, J. and Budiu, R. Mobile Usability. New Riders, 2012. ISBN-10: 0321884485
[44] https://www.rijkshuisstijl.nl/communicatiemiddelen/apps
[45] http://www.w3.org/standards/

Belastingdienst[46] bijvoorbeeld. Geadviseerd wordt de Rijkshuisstijl zoveel mogelijk toe te passen als binnen de platform specifieke richtlijnen mogelijk is.

App-iconen en het Rijksoverheid-logo. Het afzenderschap van een app van de Rijksoverheid wordt weergegeven door middel van het Rijksoverheid logo. Dit is een beeldmerk (blauw lint met onderin een speciaal voor de Rijksoverheid gestileerde versie van het rijkswapen) en een woordmerk (organisatienaam). Het lint staat bij apps altijd bovenaan, in het midden en **alleen op het launch screen**[47]. Ook een "Over deze app" pagina kan worden opgenomen in het launch screen.

Bij apps mag worden afgeweken van het standaard gebruik van het logo (beeldmerk incl. woordmerk) omdat er in de app beperkte ruimte is. De organisatienaam hoeft niet naast het logo te worden getoond, maar mag er ook onder.

Voorbeelden van het Rijksoverheid-logo in het launch screen.

Verder gelden de volgende regels vanuit de Rijkshuisstijl:

- Gebruik het logo altijd in zijn complete vorm; het lint met daarin het witte, gestileerde rijkswapen. Gebruik nooit het wapen zonder lint.
- Zet het logo centraal bovenaan en tegen de bovenkant van het schermvlak.
- De standaard basismaat van het logo wordt bepaald door het beeldmerk (lint) 44px breed x 77px hoog (1 3/4 vierkant). Op kleinere schermen wordt het beeldmerk 44px breed x 66px hoog (1 1/2 vierkant).
- De kleur van het beeldmerk is Blauw 2[48]. Het beeldmerk mag ook op een gekleurde ondergrond of foto geplaatst worden. Het woordmerk is zwart of wit, afhankelijk van de achtergrond.

[46] Contactpersoon: l.versluijs@belastingdienst.nl
[47] Een launch screen is de pagina die direct na het opstarten van de app en voor de eigenlijke hoofdpagina, wordt getoond.
[48] https://www.rijkshuisstijl.nl/basiselementen/logo/logokleuren

- Verplicht is een launchscreen dat 2,5 seconden in beeld blijft. Op dit launchscreen staat altijd het lint, de afzender en titel.

Iconen binnen een app. Binnen een app kan gebruik worden gemaakt van iconen die keuzes binnen in een app representeren. Voor Rijksoverheid publicaties zijn richtlijnen voor app-iconen en avatars[49] opgesteld waaraan iconen moeten voldoen en er is een iconenbibliotheek[50] beschikbaar om iconen en avatars voor apps en social media herkenbaar te maken als afkomstig van de Rijksoverheid. Deze basisbestanden zijn voor het gebruik in apps vanwege de hoge mate van detail niet geschikt, ze kunnen wel als basis dienen om op verder te ontwerpen. De Belastingdienst[51] bijvoorbeeld heeft een set met afgeleide iconen die bij hen op te vragen zijn.

6.2 Primaire - en specifieke doelgroepen

Ontwerp de app voor de primaire doelgroep. In het hoofdstuk Bedrijfsarchitectuur wordt hier al aandacht aan besteed ("De gebruiker staat centraal") en dit geldt zeker voor de user experience. Houd daarnaast rekening met het gebruik van de app door specifieke doelgroepen, bijvoorbeeld blinden en slechtzienden, laaggeletterden, jongeren en/of ouderen. De Web Content Accessibility Guidelines (WCAG) 2.0[52] is een door W3C opgesteld document dat bestaat uit een verzameling richtlijnen over het toegankelijk maken van content. Het volgen van deze richtlijnen maakt content ook toegankelijker voor webbrowsers en apparaten met beperkte functionaliteit zoals mobiele telefoons. In Europa is de standaard EN301 549[53] (vervanger van de open standaard Webrichtlijnen2) die gebaseerd is op de WCAG 2.0, verplicht voor websites en apps van de overheid. In Nederland zijn de EN301 549 en daarmee ook de WCAG 2.0 standaard, verplicht vanaf uiterlijk 23 september 2018. Tenslotte is in Nederland de Stichting Accessibility die kan ondersteunen bij de ontwikkeling en het beheer van toegankelijke websites en apps en een certificering toekent, het Waarmerk drempelvrij.nl[54]. Tenslotte, maak gebruik van usability testen en user experience onderzoek om te bepalen wat je doelgroep(en) belangrijk vindt en om de tevredenheid over de app en daarmee ook het gebruik van de app, te verhogen.

6.3 Specifiek- en taakgericht

Een app richt zich idealiter op de realisatie van één of enkele functionaliteiten. Maak van een app geen portaal met een waaier aan verschillende functionaliteiten en keuzes. Als richtlijn wordt 6 functionaliteiten als maximum geadviseerd. Meer functionaliteiten maken de app complex en de kans

[49] https://www.rijkshuisstijl.nl/communicatiemiddelen/apps/app-iconen-en-avatars
[50] https://www.rijkshuisstijl.nl/basiselementen/beeld/iconen-en-pictogrammen
[51] Contactpersoon: l.versluijs@belastingdienst.nl
[52] https://www.w3.org/Translations/WCAG20-nl/
[53] http://www.etsi.org/deliver/etsi_en/301500_301599/301549/01.01.01_60/en_301549v010101p.pdf
[54] https://www.accessibility.nl/audits/drempelvrij.nl-certificering

op performanceproblemen neemt toe. Begin in een app bij de primaire taak van die app, deze dient direct duidelijk te zijn. Voeg verder functionaliteit toe op basis van het verwachte gebruik.

6.4 Aantal “best practices”

Een aantal “best practices” die binnen de Rijksoverheid-apps voorkomen zijn:

- Gebruik alleen woorden in het icoon van de app als ze onderdeel zijn van het logo. Zie de volgende voorbeelden van binnen de Rijksoverheid gebruikte app-iconen.

Mobiele Hulpverlening

RWS Rooster

Berichtenbox

Intranet

Meldpunt Accijns

- Probeer de drempel voor het gebruik van de app zoveel mogelijk weg te nemen. Laat de gebruiker alleen inloggen of een pincode invoeren indien dit noodzakelijk is.
- Zorg dat dat gebruikers hooguit eenmalig een disclaimer en de gebruikersovereenkomsten moet lezen. Breng deze indien nodig onder in een apart menu.
- Vermeld in de info van de app hoe de app omgaat met de gegevens van de gebruiker.
- Gebruik een tab bar[55] om tussen de verschillende secties (primaire onderdelen) van een app te navigeren.
- Gebruik segmented control[56] opties om tussen verschillende categorieën te wisselen.
- Gebruik voor meldingen en andere dialoog met de gebruikers de Google schrijfstijl-tips[57].
- Zorg dat de dialoog de gebruiker helpt om het probleem op te lossen en formuleer meldingen op een neutrale wijze. Beperk een melding niet tot alleen een foutcode maar geef kort en bondig aan wat er fout gaat en wat een gebruiker er zelf aan kan doen of waar hij voor meer informatie terecht kan.
- Gebruik voldoende contrasterende kleuren. Status- en prioriteitsinformatie mogen nooit alleen door een kleur gepresenteerd worden, maar altijd herkenbaar door tekst of andere visuele indicatie.
- Apple heeft de Human Interface Guidelines [58] uitgebreid met een sectie voor het ontwerpen van AR-Kit apps. Deze augmented reality guidelines specificeren hoe gebruikers het beste kunnen

55 https://developer.apple.com/library/content/documentation/WindowsViews/Conceptual/ViewControllerCatalog/Chapters/TabBarControllers.html
56 https://developer.apple.com/ios/human-interface-guidelines/controls/segmented-controls/
57 https://material.google.com/style/writing.html#

communiceren met virtuele objecten, hoe dergelijke objecten geplaatst moeten worden, en de taal die developers moeten gebruiken om gebruikers te begeleiden in het uitvoeren van een taak.

[58] https://developer.apple.com/ios/human-interface-guidelines/technologies/augmented-reality/

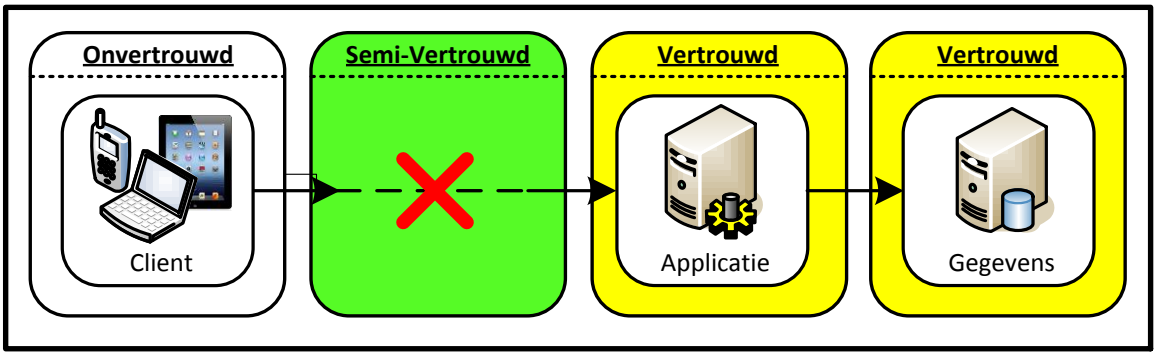
7. Infrastructuur-architectuur

Specifiek voor de infrastructuur- architectuur van apps is zonering, connectiviteit en het grote aantal ICT-componenten die deel van uitmaken van een mobiele dienst.

7.1 Infrastructurele zonering

De afbeelding in deze paragraaf is een weergave van de zonering in de infrastructuur voor een app die op een mobiel device draait en verbonden is met een back end systeem. Dit zoneringsmodel leunt sterk op het Nora beschouwingsmodel voor zonering[59].

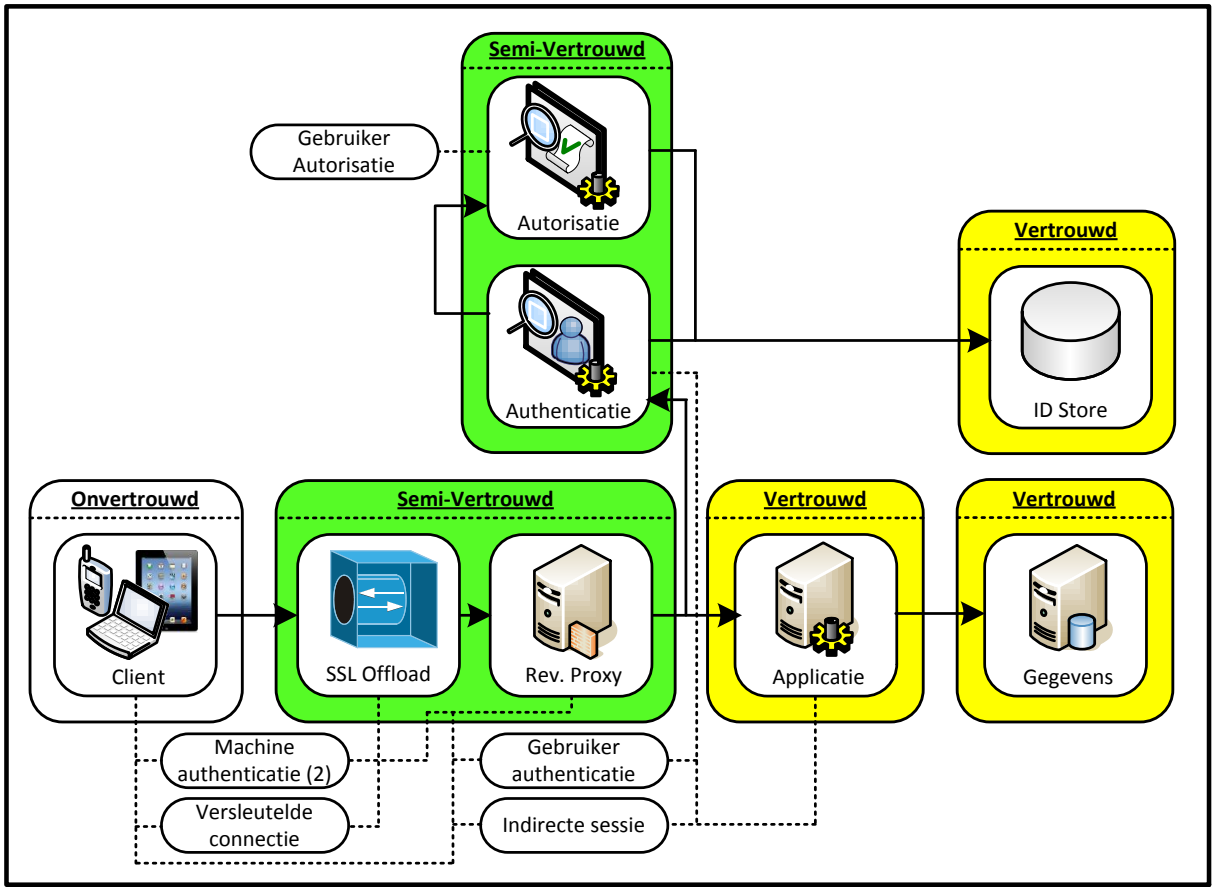
- Devices zijn nieuwe elementen in de ICT - infrastructuur met eigen spelregels.
- Zorg voor een goede OTAP omgeving inclusief representatieve devices om te testen.
- Zorg voor schaalbaarheid voor wat betreft de capaciteit van back end systemen en andere infrastructurele componenten.



Gebruikers moeten systemen uit de interne vertrouwde omgeving vanuit een externe onvertrouwde omgeving (Internet, 3G, 4G) kunnen gebruiken. Volgens het infrastructurele zoneringsmodel moet verkeer vanuit de zone Onvertrouwd naar de zone Vertrouwd mogelijk zijn. Vanwege beveiligingsredenen is het niet toegestaan dat verkeer een zone overslaat, bijvoorbeeld als een informatiesysteem een rubriceringsniveau heeft waarbij het alleen toegestaan is dat de gegevens door vertrouwde devices worden benaderd. In de BIR is opgenomen dat alleen vertrouwde devices gekoppeld mogen worden aan het vertrouwde netwerk. Vaststellen van dit vertrouwen vindt dus altijd plaats buiten deze vertrouwde zone; in een DMZ (semi vertrouwde zone).

[59] http://www.noraonline.nl/wiki/Beschouwingsmodel_zonering

De volgende afbeelding geeft weer hoe de zonering er uit ziet.



Nb. Bij gebruik van EMM\UEM-tooling kan het er enigszins anders uit zien (ook afhankelijk van de specifieke tooling). Deze afbeelding beschrijft de infrastructuur van een app die draait in een omgeving zonder dergelijke voorzieningen.

7.2 OTAP-omgeving

De ontwikkeling van mobiele oplossingen vereist een ontwikkel-, test- en acceptatie (OTA) omgeving naast de productieomgeving. Alle componenten die deel uitmaken van de keten die een mobiele oplossing tot stand brengt, moeten beschikbaar zijn in de OTA-omgeving, bijvoorbeeld een EMM\UEM-oplossing. Het is essentieel voor de ontwikkeling dat het ontwikkel- en testteam beschikt over een representatieve set van mobiele devices die een afspiegeling vormen van de door de doelgroep gebruikte mix aan devices. Het is, zeker bij apps voor het publieke domein, onmogelijk om alle soorten mobiele devices en operating system-versies “in huis” te hebben. In dergelijke situaties kan het een mogelijkheid zijn om apps op een marktconforme set devices te testen door gebruik te maken van mobiele test-oplossingen in de cloud. Deze oplossingen bieden fysieke devices die door

geautomatiseerde testen gebruikt kunnen worden. Let hier wel op of een dergelijke opzet in lijn met het beveiligings- en privacybeleid van de betreffende organisatie is.

7.3 Schaalbaarheid

Een mobiele dienst bestaat uit een groot aantal ICT-componenten die samen het succes bepalen, zoals:

- Directory-services.
- VPN-diensten.
- Databasesystemen.
- Back end systemen (mail, webservices).
- Devices
- Telecomnetwerken

Een mobiele dienst heeft impact op de capaciteit van de infrastructuur. Zorg er voor dat de netwerkinfrastructuur flexibel en schaalbaar is. Bij een mobiele dienst is de verhouding tussen devices en gebruikers essentieel anders dan bij een klassieke werkomgeving. Bij deze laatste is er een vast aantal werkplekken waarop de achterliggende infrastructuur berekend en geschaald kan worden. Bij de mobiele diensten zijn er meerdere devices per gebruiker, met veel variatie in aantallen. Dit is moeilijker voorspelbaar en planbaar. Een goede monitoring en anticiperend vermogen op capaciteit binnen de gehele infrastructuur is een vereiste voor mobiele diensten. Als bijvoorbeeld E-mail op mobiele devices aangeboden wordt, is van te voren belangrijk om na te gaan of het huidige mail systeem hier op geschaald is. De belasting van het mailsysteem kan twee tot drie keer toenemen aangezien gebruikers van één naar twee of drie devices gaan. Houd ook rekening met sterke toename van de netwerkbelasting, zeker als men gebruik gaat maken van VPN-connectiviteit.

7.4 Connectiviteit

Bij het gebruik van apps op een mobiel device is connectiviteit essentieel om de gegevensuitwisseling tussen de app en de achterliggende backend systemen te kunnen realiseren. Voor apps is dit essentieel anders dan voor applicaties in een klassieke enterprise-omgeving. Er zijn twee vormen van mobiele connectiviteit:

- WiFi bestaat er in diverse technische varianten met elk hun eigen kernmerken qua bereik en capaciteit. WiFi kan gecontroleerd worden aangeboden in een bedrijfsomgeving. Hierdoor is er invloed op deze beide parameters. Bij WiFi in de openbare ruimte (Hotspots) en huiselijke omgeving is deze invloed er niet. De steeds hoger wordende penetratie van WiFi in de huiselijke omgeving heeft een nadelige invloed op het bereik en de capaciteit van een thuisaansluiting. Immers het signaal houdt niet op bij de

buitenmuren en steeds meer netwerken willen gebruik maken van de beperkte frequentieruimte die voor WiFi beschikbaar is.

- De landelijke mobiele netwerken bieden datatransmissie aan op basis van 3G en 4G technologie. Binnen deze netwerken is het slechts beperkt mogelijk bedrijfsmatige beheerde omgevingen af te nemen. Daarnaast is bereik niet gegarandeerd. De meeste providers leveren weliswaar een landelijke dekking, echter gebaseerd op gebruik buitenshuis. Indoor dekking wordt primair bepaald door de constructie van het gebouw.

Belangrijke parameters bij deze twee vormen van connectiviteit zijn bereik en capaciteit. Beide zijn randvoorwaardelijk om een goede user experience te kunnen bieden. Afhankelijk van de functionaliteit en doelgroep van de app dient er ook rekening mee gehouden te worden dat connectiviteit niet gegarandeerd is. Bepaalde apps zullen dus ook zonder een connectie met hun back end, dus offline, moeten kunnen functioneren. Bij apps die met latency-gevoelige data werken (bijvoorbeeld beeld en geluid) is een voldoende netwerkcapaciteit een vereiste.

Gebruik van (commerciële) connectiviteit is niet gratis. Houdt er, zeker bij publieke apps, rekening mee dat de benodigde transmissiecapaciteit in overeenstemming is met het doel van de app en de gebruikersgroep. Deze gebruikskosten liggen immers bij de gebruiker van de app en niet bij de aanbieder.

Het is belangrijk bij het testtraject ook de stabiliteit van de app te testen onder wisselende bereikbaarheidsscenario’s zoals een kwalititatief slechte verbinding, lage bandbreedte enz.

7.5 Cloud

Het gebruik van clouddiensten en -technieken neemt toe. De Rijksoverheid heeft een terughoudend beleid t.a.v. het gebruik van publieke clouddiensten. Via het inrichten van overheidsdatacentra worden de interne ICT-voorzieningen ingericht als een private cloud. Voor de ontwikkeling en beheer van apps kunnen desondanks wel clouddiensten of -technieken worden ingezet, waarbij dan wel een zorgvuldige afweging moet worden gemaakt of hier publieke of private cloud wordt gebruikt, zoals:

- Welke gegevens ga ik verwerken; hoe vertrouwelijk of privacygevoelig zijn deze.
- Waar vind deze verwerking geografisch plaats.
- Aan welke wetgevingen ben ik als opdrachtgever dan gehouden.
- Welke waarborgen kunnen er met de aanbieder worden overeengekomen; welke contractuele afspraken zijn er mogelijk.
- Is er een goede exit-strategie mogelijk.

Vanuit het Ministerie van Binnenlandse Zaken en Koninkrijkrelaties is er door DGOO/CIO-Rijk een handreiking dataopslag gemaakt die hier behulpzaam bij kan zijn. Deze is verkrijgbaar via het secretariaat [60]van DGOO.

[60] secretariaatCIORijk@minbzk.nl

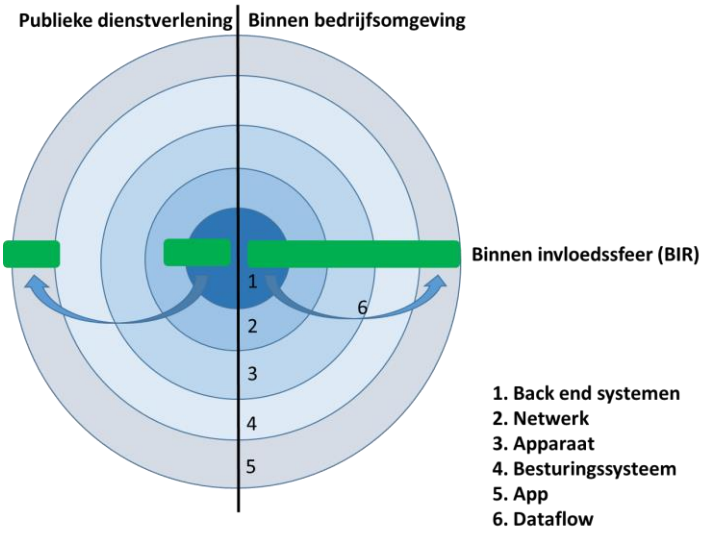
8. Beveiliging

Het aanbieden van diensten via een app, zeker in het publieke domein, brengt diverse uitdagingen met zich mee op het gebied van beveiliging. Het is zaak de gegevens die met de app en gebruiker worden gedeeld goed te beveiligen. Deze beveiliging is vereist, ongeacht de vraagstelling of de Rijksoverheid de eigenaar of een bewerker van de gegevens is.

- Voer per app een risicoanalyse uit en kies de juiste mix aan beveiligingsmaatregelen voor de app.
- Publieke apps dienen intrinsiek veilig te zijn. Voor enterprise apps kan er eventueel gebruik worden gemaakt van EMM\UEM-voorzieningen.
- Bij publieke apps is er een reëel risico op nagemaakte of gemodificeerde varianten (cybercriminaliteit), houd hier rekening mee.

8.1 Beveiliging en de Rijksoverheid

Net als iedereen dient ook de overheid zich aan de wet te houden. Om aan de wetgeving te kunnen voldoen is binnen de overheid de Baseline Informatiebeveiliging Rijk (BIR)[61] in gebruik. De BIR is een verzameling van kaders en richtlijnen waar alle aspecten met betrekking tot ICT-dienstverlening (bedrijfsvoering, processen, personeel en infrastructuur) aan dienen te voldoen.



Bij enterprise apps is er een end-to-end invloed op de beveiligingsmaatregelen, bij apps met gebruikers in het publieke domein is dit niet het geval. Er is geen of slechts minimale controle over het apparaat, over het besturingssysteem en over het netwerk, vanaf het moment dat de gegevens het overheidsnetwerk verlaten en via de publieke datanetwerken getransporteerd worden. Dit levert een spanningsveld op met deze handreiking met betrekking tot informatiebeveiliging, vooral de BIR.

[61] http://www.earonline.nl/index.php/Overzicht_Baseline_Informatiebeveiliging_Rijksdienst_(BIR_2012)

Naast de BIR zijn er nog diverse andere kaders die relevant zijn bij de te nemen maatregelen rondom informatiebeveiliging. Dit zijn in ieder geval:

- Algemene Verordening Gegevensbescherming (AVG)
- Voorschrift Informatiebeveiliging Rijksdienst (VIR) 2007
- Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2013 (VIR-BI)
- BIR 2012 TNK / BIR 2017
- NEN-ISOSEC 27001
- NEN-ISOSEC 27002
- Nederlandse Overheid Referentie Architectuur (NORA) IB-Katern
- CIP-publicatie "Grip op Secure Software Development (SSD) Beveiligingseisen voor mobile apps"[62]
- NCSC publicatie "ICT-beveiligingsrichtlijnen voor mobiele apps"[63]

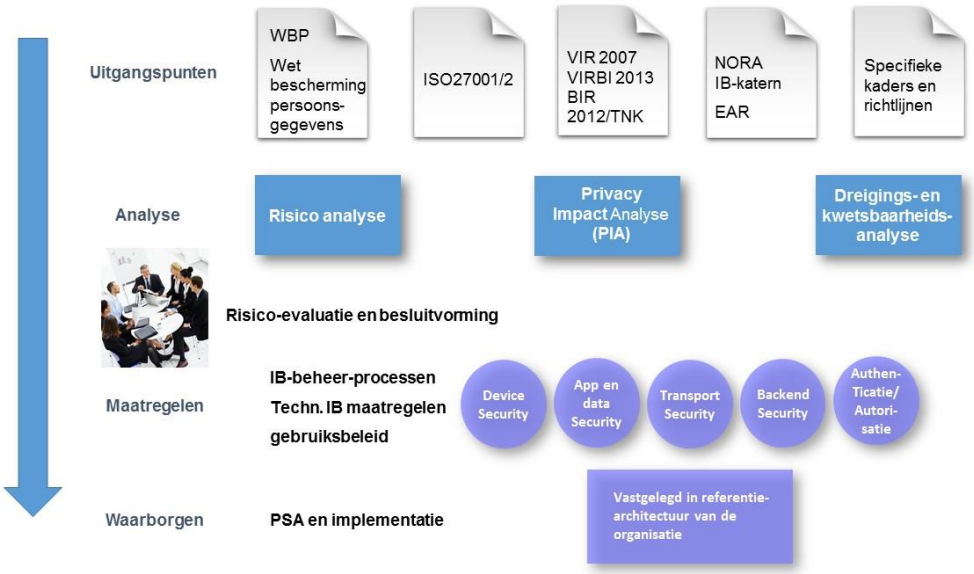
8.2 Maatregelen op basis van een risicoanalyse

De opdrachtgever van de app bepaalt op basis van een risicoanalyse hoe gegevens beschermd dienen te worden en waartegen. Op basis van deze analyse kan, bij voorkeur in samenwerking met de leverancier(s) van de app en/of andere ICT-voorzieningen, de juiste set van de benodigde maatregelen worden vastgesteld. Vragen die belangrijk zijn in dit traject:

1. Hoe belangrijk/vertrouwelijk is de informatie die in een app wordt verwerkt of gepresenteerd?
2. Wie is eigenaar van deze informatie?
3. Welke risico's zijn er?
4. Welke aanvullende wettelijke of andere regelingen zijn op deze gegevens of de verwerking ervan van toepassing?
5. Op welke platformen draait de app? Wie is de eigenaar van deze apparaten?

In de volgende afbeelding wordt dit proces weergegeven.

[62] http://www.cip-overheid.nl/wp-content/uploads/2016/03/20160225_Grip_op_SSD_Mobile_apps_Beveiligingseisen_v1.00.pdf
[63] https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-mobiele-apps.html



Er zijn drie gouden regels die gelden voor apps die privacygevoelige gegevens bevatten. Het verdient aanbeveling om deze regels actief mee te delen aan de gebruiker, bijvoorbeeld door een informatie- of gebruiksvoorwaarden mededeling bij het eerste gebruik van een app te tonen met daarin het volgende:

1. Gebruik altijd de originele software op het apparaat en de meest recente versie daarvan (besturingssysteem).
2. Gebruik altijd de officiële app store van het platform of gebruik bij apps voor intern gebruik de interne Enterprise App store of distributievoorzieningen van de eventuele EMM\UEM[64]-tooling.
3. Beveilig de toegang tot het apparaat (met bijvoorbeeld een toegangscode).

Bij het gebruik van apps binnen de eigen bedrijfsomgeving kunnen meerdere maatregelen worden getroffen om de veiligheid van het gebruikte device te waarborgen. Denk hier aan het gebruik van EMM\UEM-voorzieningen die strikte device policies en bijvoorbeeld een remote wipe kunnen afdwingen en strikte regels rondom toegestane versies van de systeemsoftware. Indien een EMM\UEM wordt toegepast; lever zo mogelijk het apparaat beveiligd uit aan de gebruiker of gebruik OS-specifieke activatievoorzieningen om ongeautoriseerde toegang of aanpassingen te voorkomen.

Belangrijke uitgangspunten voor beveiliging met betrekking tot apps:

- Publieke apps dienen intrinsiek veilig te zijn; er kan niet worden teruggevallen op MAM, MDM of MIM[65]-hulpmiddelen. Een gebruiker moet er van uit gaan dat de app die hij installeert zonder aanvullende maatregelen of instellingen gebruikt kan worden.

[64] EMM= Enterprise Mobility Management; UEM= Uniform Endpoint Management, zie voor uitleg hoofdstuk Beheer en distributie
[65] MAM = Mobile Application Manamagement; MDM = Mobile Device Management; MIM = Mobile Information Management, zie voor uitleg hoofdstuk Beheer en distributie.

- Maak zo veel als mogelijk gebruik van de voorzieningen van het device en het platform om de beveiliging van apps te verbeteren. Betrek de benodigde IB-maatregelen ook bij een eventuele keuze tussen native, hybride of web apps.
- Versleutel de gegevens. Dit geldt voor zowel de gegevens die op het device opgeslagen worden, als voor het transport tussen de app en de back end systemen via het netwerk.
- Bepaal de sterkte van de sleutel en de cryptografische algoritmen aan de hand van de gevoeligheid en de levensduur van de informatie.
- Bepaal de maximale footprint van de data op het device. Een zero footprint is een ideaal, maar in de praktijk vaak niet haalbaar. Dit zou betekenen dat een app geen data op een device opslaat. Maak een juiste afweging welke data lokaal op het device opgeslagen moet worden, rekening houdend met factoren als performance, belasting back office en dataverbinding en online- en offlinegebruik.
- Voorzie de app van een ‘data clean up’ functie waardoor de app de data die niet langer benodigd is, actief verwijdert van het device.
- Toegang tot privacygevoelige gegevens vereist een afdoende vaststelling van de identiteit van de gebruiker. Kies hiervoor het meest geschikte middel binnen de vigerende authenticatiemethoden. Adopteer tijdig nieuwe authenticatiestelsels wanneer deze voor de doelgroep beschikbaar komen.
- Voor bepaalde informatie of bedrijfsprocessen kan het relevant zijn dat slechts een bepaalde set devices (bijvoorbeeld goedgekeurde of bedrijfseigen toestellen) kunnen worden gebruikt. In dat geval kan device-authenticatie een zinvolle maatregel zijn. Hiervoor worden unieke kenmerken van het apparaat gebruikt zoals een uniek identificatienummer of geïnstalleerde certificaten.
- Voor apps die met privacygevoelige informatie werken is het belangrijk om de toegang tot de app af te schermen en niet te vertrouwen op de afscherming van het device. Denk hierbij aan een toegangscode of vingerafdruk voor toegang tot de app. Dit is vooral bescherming tegen medegebruikers van het device bij dagelijks gebruik en niet tegen compromittering en/of hacken van het device.
- Denk na over de data die een app op het device bewaart in relatie tot voor de devices gebruikte back-strategie. Mag deze data wel of niet in een backup meegemomen worden en waar kan deze dan terecht komen? Backups kunnen lokaal gemaakt worden (via een USB-kabel) of naar de cloud.
- Bouw echtheidskenmerken in. Apps worden steeds vaker nagemaakt of gemanipuleerd. Het is erg moeilijk om een nagemaakte app van een echte app te onderscheiden of om maatregelen tegen niet-authentieke apps te ondernemen.
- Gebruik geregistreerde beeldmerken zoals het Rijksoverheidslogo (het blauwe lint) op essentiële plaatsen in de app (zie het hoofdstuk User experience). Onrechtmatig gebruik van een dergelijk beeldmerk vormt een solide juridische basis om zaken uit de de publieke app stores te laten verwijderen.

- Scan regelmatig de diverse publieke app stores op mogelijke onrechtmatige varianten van de app. Dit scannen kan een handmatig of geautomatiseerd proces zijn, afhankelijk van de geïdentificeerde risico's.
- Definieer lifecyclemanagement voor bedrijfsdevices. Devices kennen vaak maar een beperkte support periode door de fabrikant m.b.t. levering van OS-updates en security-patches. Zorg er voor dat alle actieve devices binnen de support van de fabrikant vallen.

9. Beheer en distributie

Het beheer en de distributie van mobiele apps is op een aantal punten anders dan het beheer van traditionele applicaties op een vaste werkplek. Tegelijkertijd zien we de ontwikkeling om het beheer van de vaste werkplek en mobiele devices zo uniform mogelijk te organiseren. Na de introductie van Enterprise Mobility Management (EMM) suites die het mogelijk maken om apps, mobiele devices, draadloze netwerken en aanverwante services te managen is er nu de trend naar Uniform Endpoint Management (UEM) . Wat betreft de (door)ontwikkeling van apps, de gebruikte EMM of UEM suites en het distributiekanaal, kunnen keuzes worden gemaakt. Deze zijn in dit hoofdstuk beschreven. Verder heeft de keuze voor publieke apps of interne rijksoverheid apps impact op de te volgen beheerstrategie.

9.1 (Door) ontwikkelen van apps

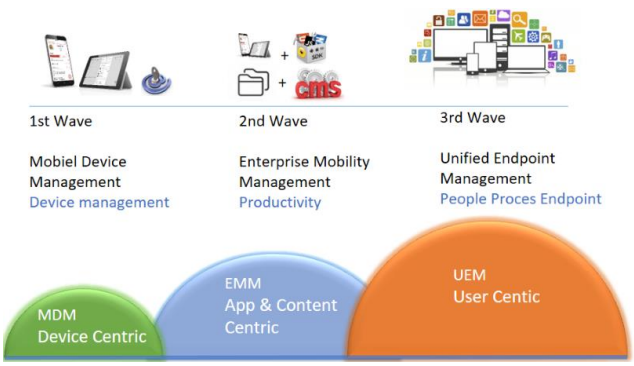
Specifiek voor de (door)ontwikkeling van apps is het snel en frequent opleveren van nieuwe versies naar de productieomgeving. Een DevOps werkwijze, waarbij beheer en ontwikkeling samen verantwoordelijk zijn voor de werking en de ontwikkeling van een dienst, is hiervoor heel geschikt.

- Laat de app signen met een door de Rijksoverheid uitgegeven certificaat.
- Zorg voor strategische afstemming tussen de EMM\UEM inrichting en de werkplek architectuur.
- Kies een distributiekanaal op basis van de gebruikersgroep van de app.

Om de integriteit van de app in het Overheidsdomein te waarborgen is het signen met een door de Rijksoverheid uitgegeven of organisatie specifiek certificaat essentieel. Bij het signen wordt een legitieme status toegekend aan de app waarmee deze “integer” kan worden aangeboden aan de eindgebruiker. Laat de app niet signen door een commerciële partij, dit is verwarrend voor de gebruiker. Neem in de app wel een link naar de website van de ontwikkelaar op.

9.2 Unified endpoint Management (UEM)

Unified Endpoint Management (UEM) is de doorontwikkeling van Enterprise Mobility Management (EMM). Waar EMM het mogelijk maakt om apps, mobiele devices, draadloze



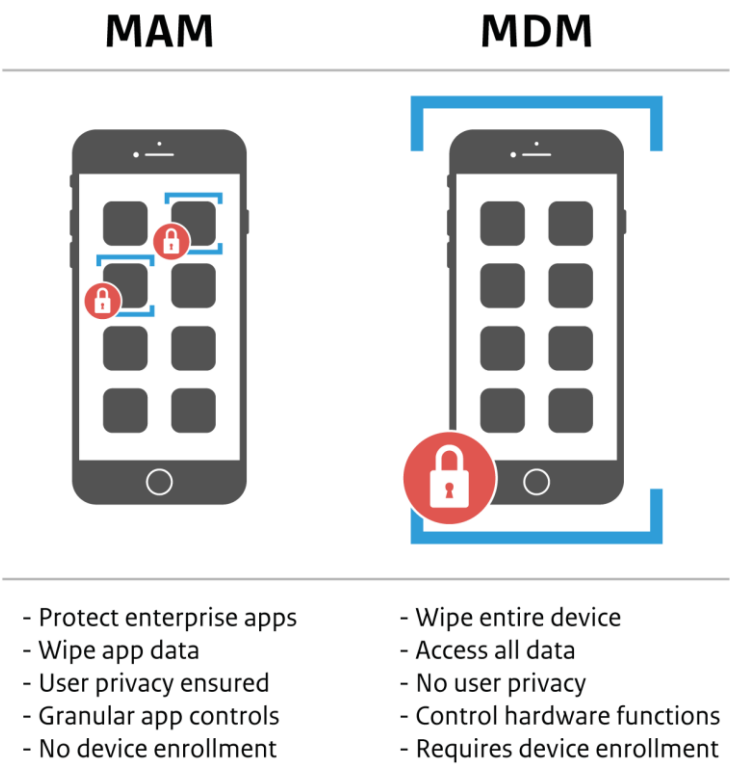
netwerken en aanverwante services voor medewerkers, te managen, gaat UEM een stap verder. UEM geeft de mogelijkheid om een grote verscheidenheid van apparaten met verschillende verschijningsvormen en besturingssystemen zoals PC's en laptops, tablets en smartphones, en ook wearables en Internet of Things (IoT) eindpunten centraal te beheren. Net als EMM is een UEM oplossing een samenvoeging van Mobile Device Management (MDM), Mobile Application Management (MAM) en Mobile Information Management (MIM) .

Mobile Device Management (MDM) stelt de organisatie in staat zowel privé als vanuit het bedrijf verstrekte devices te laten vergrendelen of te wissen en om de gebruiker te helpen met de configuratie-instellingen van zijn device.

MDM-gebaseerde oplossingen hebben echter twee belangrijke beperkingen:

- **Beperkt bereik.** Via MDM kunnen alleen apps aan de interne medewerkers worden gedistribueerd, niet aan de burger. MDM wordt meestal ingezet voor devices die eigendom zijn van de organisatie. Tenslotte kan er slechts één organisatie het device managen. Dit is een beperking wanneer rijksambtenaren bij meerdere ministeries werkzaam zijn.
- **Gebrek aan beheerfuncties voor apps.** De app-distributie functies in MDM zijn geschikt voor relatief simpele apps en niet geschikt voor complexe omgevingen waar bijvoorbeeld gebruikersgroepen over een eigen set aan apps moeten beschikken.

Mobile Application Management (MAM) richt zich op het beveiligen en beheren van apps en gegevens binnen de app, los van het device en is geschikt voor privé-devices van medewerkers. Via een MAM platform kunnen apps ook gedistribueerd worden op elk apparaat, ongeacht of een app wordt beheerd via een MDM. Een nadeel is dat MAM zonder MDM geen tegenwicht biedt aan de kwetsbaarheden van het operating system, wat alsnog kan leiden tot kwetsbare apps. MAM biedt verder de mogelijkheid om diensten te leveren buiten het eigen verzorgingsgebied van de IT-leverancier en rijksbrede apps te ontwikkelen en te distribueren. Binnen deze “app centric” benadering moet een goede MAM oplossing de volledige app-levenscyclus ondersteunen met o.a. de volgende functies:



- Het toevoegen van apps aan het systeem (“app-onboarding”).
- Het inspecteren van apps om ervoor te zorgen dat ze veilig zijn (“app-inspectie”).
- Het beveiligen van apps met beleid (“app-bescherming”).
- Het verspreiden van apps naar alle gebruikers (“app-deployment”).
- Bepalen of apps worden gebruikt en het verkrijgen van de gebruiker opmerkingen (“app-analytics”).
- Bijwerken apps op regelmatige basis (“app-administratie”).
- Per app VPN-functionaliteit.

Mobile Information Management (MIM). Het idee achter MIM is het veilig kunnen aanbieden van Rijksoverheids-informatie. Hierbij kan men denken aan file sharing van zowel data in de cloud als data binnen bestaande domeinen (bijvoorbeeld netwerk fileshares), gepresenteerd naar een mobiele front end, of het kunnen benaderen van SharePoint sites of home directories. Er zijn reeds producten op de markt die interfaces hebben naar bekende Enterprise Content Management oplossingen zoals Filenet, IBM connection en Hummingbird. MIM oplossingen maken gewoonlijk gebruik van een veilige container rond gevoelige data, deze is encrypted en alleen geautoriseerde gebruikers kunnen er bij. Om MIM optimaal in te zetten moet identity management er onderdeel van uit maken.

De laatste jaren komen er steeds meer Content Collaboration Platformen op de markt, voorheen ook wel aangeduid als Enterprise File Sync And Share (EFSS). Deze oplossingen bestaan uit een verzameling van tools en hulpmiddelen die zorgen dat medewerkers op elk gewenst moment toegang hebben tot (gedeelde) content en veilig kunnen samenwerken waarbij de controle op de content waar deze zich ook bevindt, behouden blijft. Door het analyseren van monitoringinformatie kunnen verdachte patronen herkend worden en eventuele veiligheids lekken achterhaald worden. Zeker in het kader van EU’s Genaral Data Protection (GDPR) DPR monitoren Analytics kunnen deze systemen een toegevoegde waarde hebben.

9.3 Keuze voor een EMM/UEM oplossing

Er zijn verschillende redenen om een EMM of UEM oplossing te gebruiken zoals het op afstand willen beheren van devices, het afdwingen van het gebruik van een wachtwoord op devices en de distributie van apps. Deze oplossing wordt veelal gebruik ingeval er sprake is van interne apps die een hoog beveiigingsriscico hebben. Indien de doelgroep burgers is, is deze beheeroplossing niet toepasbaar. De volgende aspecten zijn relevant bij de keuze voor een EMM of UEM oplossing.

- **Compleetheid.** Een goede EMM/UEM oplossing biedt niet alleen MDM-mogelijkheden om apparaten te beveiligen en te beheren, maar zorgt ook voor het uitrollen van apps en het beheren en beveiligen via MAM en functionaliteit voor identiteits- en toegangscontrole.
- **Volwassenheid.** EMM/UEM zelf is inmiddels een mainstream product en vormt vaak een onderdeel van de bredere dienstverlening. Dit houdt in dat een volwassen EMM/UEM-

oplossing binnen één overkoepelende beheerconsole te managen is. Let er op dat de leverancier een roadmap voor de toekomst heeft klaarliggen en eerdere acquisities om de EMM/UEM -functionaliteit aan te vullen, goed heeft geïntegreerd.

- **Gemakkelijk uit te rollen.** De eenvoud in deployment verschilt tussen de diverse aanbieders. Dit is van belang omdat de behoeften per organisatie verschillen en er ook op het niveau van teams en individuen andere eisen kunnen gelden. Dat vraagt om een brede inzet van verschillende policies en tools en dus om een flexibele oplossing.
- **Schaalbaarheid.** Zowel de werkgerelateerde inzet van mobiele devices als het aantal apparaten per werknemer groeit. Een EMM/UEM-oplossing moet in de toekomst kunnen meeschalen met de groei van het aantal devices. Let daarbij op de kosten.
- **Licentiestructuur**. Een pakket moet de keuze bieden tussen een user- of een device-licentiestructuur. Kies de licentiestructuur die het beste aansluit bij het bedrijfsmodel. Vanwege de toename van het aantal mobiele devices per persoon is de user based licentiestructuur vaak het efficiëntste.
- **Reputatie leverancier.** Hoewel een aantal EMM/UEM -leveranciers inmiddels een goede naam heeft opgebouwd, zijn er flink wat spelers die pas net komen kijken en nog geen of weinig cases kunnen laten zien. Kijk daarom goed naar de reputatie van het bedrijf, naar de branches waarin ze klanten bedienen en naar de ervaringen van deze partijen. Een mogelijke bron is het Magic Quadrant dat Gartner ieder jaar publiceert. Een multilayer concept is in sommige gevallen een goede oplossing om minder afhankelijk te zijn van één leverancier.

9.4 Aantal “best practices”

Tot slot een aantal “best practices”op het gebied van EMM/UEM:

- **Beveiliging versus gebruiksvriendelijkheid.** Zorg dat de gebruiksvriendelijkheid en beveiliging in evenwicht zijn. Als de policies te strak worden ingesteld, gebruiken medewerkers de functionaliteiten niet en gaan ze er omheen werken. Door gebruik te maken van de laatste technologieën kan de gebruiksvriendelijkheid verbeterd worden. De mogelijkheid om data te ontsluiten via vingerscan bijvoorbeeld, verhoogt de gebruikersbeleving aanzienlijk. Het zal per organisatie echter bekeken moeten worden of deze technieken toegepast kunnen worden in verband met het vigerende beveiligingsbeleid. Raadpleeg de zogenaamde inzet adviezen van het NBV[66] over de inzetbaarheid van EMM/UEM -omgevingen binnen de Rijksoverheid. Houd tenslotte ook rekening met de dataclassificatie van de informatie bij de keuze van de EM-oplossing.

66 https://www.aivd.nl/onderwerpen/informatiebeveiliging/inhoud/beveiligingsproducten/inzetadviezen

- **Toegangscontrole.** Beperk het gebruik van verschillende wachtwoorden voor apps tot een minimum. Sommige EMM/UEM -leveranciers bieden de mogelijkheid om alle apps binnen de beveiligde omgeving met hetzelfde wachtwoord te beveiligen. De beste beleving wordt gerealiseerd als single sign-on (SSO) ingeregeld kan worden voor de toegang tot apps.
- **Beheerorganisatie.** De ondersteuning van mobiele diensten is wezenlijk anders dan de ondersteuning van bijvoorbeeld Windows-werkplekken. Indien de gebruiker een probleem heeft met zijn device of app is remote ondersteuning lastig. Het is dan ook aan te bevelen om een service desk in te richten voor ondersteuning voor mobiele devices of deze te integreren met de bestaande. Storingen aan mobiele diensten kunnen complex zijn. De dienst is afhankelijk van vele ICT-componenten en vaak verschillende ondersteunende beheerteams. Mobility-diensten vereisen een interne keten gestuurde aanpak. Het is dan ook aan te bevelen de diverse mobility-disciplines in één afdeling onder te brengen (bijvoorbeeld in eenmobile competence center).
- **Uitrol mobiele devices.** Het uitleveren van mobiele devices aan de eindgebruikers is een tijdrovende klus. De gebruiker speelt hier een essentiële rol omdat er een persoonlijk account nodig is om apps van de verschillende leveranciers te installeren vanuit de verschillende app stores. Bij veel organisaties moet de gebruiker daarom zelf de configuratie van het device uitvoeren. Als de uitrol procedure niet gebruiksvriendelijk is, geeft dit in de praktijk veel problemen en veel druk op de beheerorganisatie of de servicedesk.
- **Automatiseren uitrol.** Er zijn momenteel oplossingen beschikbaar om de uitrol te verbeteren en de doorlooptijd van het uitrol-proces te verkorten, bijvoorbeeld het Apple Deployment Enroll Program (DEP) of het Knox Mobile Enrollment Program van Samsung. Recent heeft Google “Zero touch enrollment” geintroduceerd. Alle oplossingen zijn erop gericht om de uitrol van het MDM en de apps sneller te laten verlopen met minimale inspanning van de gebruiker. Als DEP samen met het Volume Purchase Program van Apple gebruikt wordt , is het mogelijk om apps zonder het gebruik van een Apple-ID te installeren.
- **Kennis delen.** De markt van EMM/UEM oplossingen is nog relatief jong en de kennis ervan in Nederland is schaars. Ongeacht welke oplossing gekozen wordt, is het beschikbaar hebben van kennis binnen de organisatie van essentieel belang. Denk hierbij ook aan workshops en trainingen van gebruikers om de adoptie van mobiele diensten te verbeteren.

9.5 Distributiekanalen

Er zijn verschillende manieren waarop een app kan worden verspreid naar gebruikers binnen en buiten de Rijksoverheid.

Publieke app stores (Apple Store of Google Play) zijn de meest bekende verzamelplaatsen voor het downloaden van apps voor mobiele devices. De Dienst Publiek en Communicatie[67] (DPC) van het Ministerie van Algemene Zaken is het centraal aanspreekpunt voor het gebruik kunnen maken van centrale ontwikkel-accounts (zowel voor Android, iOS, BlackBerry als Windows) op naam van rijksoverheid.nl. DPC laat ontwikkelpartijen gebruik maken van distributie-certificaten en zorgt voor het beheer van deze certificaten. Het ministerie van Defensie vormt hierin een uitzondering en heeft een eigen account.

Voordelen van publieke app stores ten opzichte van enterprise app stores:

- **Gebruiksvriendelijkheid.** Integratie van de app store met het operating systeem.
- **Beschikbaarheid(24*7).** Hoge mate van betrouwbaarheid en een wereldwijd bereik.
- **Zichtbaarheid.** Over de hele wereld te benaderen. Voor publieke apps de “way to go”.
- **Doelgroep.** Mogelijkheid om apps aan te bieden aan partijen buiten het eigen verzorgingsgebied (interdepartementaal).

Nadelen van publieke app stores ten opzichte van enterprise app stores:

- **Beheerbaarheid.** Er is geen controle over de apps; een app kan uit de app store worden verwijderd, maar kan niet gemakkelijk worden ingetrokken van de apparaten die het al hebben gedownload. De consequentie is dat elke gewenste (toegangs)controle moet worden ingebouwd in de app zelf. Ook geldt dat updates kunnen worden gepubliceerd, maar dat het niet gegarandeerd is dat de eindgebruiker ze ook daadwerkelijk installeert.
- **Zichtbaarheid (voor de enterprise apps).** Publieke app stores kunnen enterprise apps hosten. De app wordt dan zichtbaar voor iedereen. Wanneer de enterprise app een login en andere veiligheidsmaatregelen bevat, is dit niet aan te raden omdat deze informatie gebruikt kan worden door hackers.
- **Flexibiliteit.** Het volledige intake proces van een app door de leverancier van een app store duurt enige dagen wat een nadelig effect heeft op de levertijd van een app. Google‘s goedkeuringsproces is meer reactief (malafide/ slechte apps worden uit de winkel genomen), terwijl dat van Apple meer proactief is (screening vooraf). App stores richten zich vooral op branding en distributie en leveren niet de benodigde management-mogelijkheden die nodig zijn om apps te beheren tijdens hun volledige levenscyclus.
- **Security.** Malware-apps duiken regelmatig op in de publieke app stores. Hier onder verstaan we nagemaakte apps en apps die ongewenste software op je device installeren.

Enterprise app store als onderdeel van EMM/UEM**.** Voor veel organisaties is een enterprise app store als onderdeel van een EMM/UEM -oplossing het optimale mechanisme om eigen ontwikkelde apps te catalogiseren en te distribueren. Hierbij kunnen ook links naar de publieke app stores opgenomen

67 https://www.rijksoverheid.nl/ministeries/ministerie-van-algemene-zaken/inhoud/organisatie/organogram/dienst-publiek-en-communicatie

worden. Deze app store kan integreren met bestaande enterprise Identity Management (IdM) en Identity & Acces Management (IAM) systemen, waardoor alleen de voor een gebruiker(groep) relevante apps worden gepubliceerd.

Voordelen van een enterprise app store als onderdeel van een EMM/UEM:

- Een enterprise app store vormt een catalogus voor de apps van de organisatie en is een goede methode voor de presentatie en het testen van bèta-versies van apps. Het stelt organisaties bijvoorbeeld in staat om apps alleen te presenteren aan een groep testers.
- Meer controle over het life cycle management. Er kan gekozen worden voor push- of pull-mechanismen voor de distributie, geforceerde updates en vaak ook verwijderen van apps van een device.
- Bieden een centraal portaal voor de gebruiker om alle apps die nodig zijn voor het werk te kiezen en te installeren.
- Controle over de apps die in de app store komen.
- Gebruiker hoeft geen goedkeuring te geven voor het vertrouwen van zelf ontwikkelde enterprise apps.

Nadelen van een enterprise app store als onderdeel van een EMM/UEM:

- De app store is onderdeel van de EMM/UEM -oplossing, bij eventuele migratie naar een andere EMM/UEM -oplossing moet dus ook van app store gewisseld worden.
- Het is niet mogelijk apps te verspreiden op andere devices dan die door de eigen organisatie worden beheerd.
- De functionaliteit van de app store is meestal niet zo uitgebreid; meestal een catalogus met apps zonder mogelijkheid voor Substores. Voor kleine organisaties met enkele apps kan dit voldoende zijn.
- Indien men buiten het eigen verzorgingsgebied diensten wil leveren kan dit moeilijk realiseerbaar zijn vanwege de mogelijke integratie met de organisatiegebonden IAM- en IdM-systemen.

Autonome enterprise app store. Een autonome enterprise app store is een app store voor medewerkers met inbegrip van gebruikers met een eigen device, klanten en partnerbedrijven met als doel bedrijfsmatige en beveiligde mobiele apps aan te bieden en te installeren. Deze gespecialiseerde oplossingen hebben geen mobile device management nodig en bieden vaak uitgebreide mogelijkheden voor gebruikersfeedback en ratings, en leggen de nadruk op het gebruiksgemak. Tevens zijn er oplossingen die een set van beveiligings- en beheermogelijkheden bezitten voor het beheer van elke fase van de levenscyclus van de app.

Voordelen van een autonome enterprise app store:

- Door de juiste apps toe te wijzen aan de juiste afdelingen en groepen in de organisatie is men er altijd zeker van dat alle medewerkers, klanten en partnerbedrijven de nieuwste versies van hun apps hebben.
- Mogelijkheid om apps aan te bieden aan partijen buiten het eigen verzorgingsgebied (interdepartementaal).
- Meestal gespecificeerde producten die veel mogelijkheden bevatten voor efficiënte distributie (catalogus, review mogelijkheden). Zeker indien meerdere organisaties bediend moeten worden.
- Controle over de apps die in de app store komen.

Nadelen van een autonome enterprise app store:

- Extra technisch en functioneel beheer. Niet geïntegreerd met MDM- of EMM/UEM -systeem.
- Extra licentie kosten.
- Geen mogelijkheid om apps te beheren. Geen push- en pull-mogelijkheden indien de oplossing niet in combinatie met MDM gebruik wordt.

9.6 Afwegingskader app stores

Om te bepalen welke app store past bij de mobiele strategie zijn de volgende vragen een leidraad:

- Wat is de doelgroep: burgers en/of bedrijven, rijksambtenaren of een specifiek ministerie of uitvoeringsorganisatie? Zijn alle eindgebruikers te bereiken op basis van een doelgroep?
- Moet de app beheerd worden tijdens de gehele beheercyclus? Moeten distributie en rollback zonder inzet van de eindgebruiker mogelijk zijn?
- Wordt de app gepushed of wordt de eindgebruiker in staat gesteld zelf te bepalen de app op te halen (pull-mechanisme) in een centrale app store (centrale/enterprise of publieke store)?
- Wat is de dataclassificatie; open data, Departementaal Vertrouwelijke informatie of hoger?
- Zijn er licentiekosten verbonden aan de uitrol?

In een tabel weergegeven ziet dit er als volgt uit:

Gevraagde functionaliteit	Enterprise app store (via EMM/UEM)	Publieke app store	Autonome Enterprise app store (zonder EMM/UEM)
Doelgroep Burgers/ bedrijfsleven	--	++	-
Doelgroep Departementale publicatie	++	=	++
Doelgroep Interdepartementaal beschikbaar	-	=	+
Zichtbaarheid naar doelgroep (vindbaarheid)	++	-	++
Doorlooptijd plaatsingsprocedure	+	=	+
Beheerbaarheid lifecycle app (push /pull)	+	-	=
Beoordelingsmogelijkheid	+	++	++
Beveiligde (interne) apps	++	- -	+
Test mogelijkheid	+	-	++
Branding	=	-	+
kosten publicatie	+	-	-
Geïntegreerde beveiliging mogelijkheid	+	-	=
Uitgebreide mogelijkheden voor differentiatie (categorieën)	+	=	++
Licentie-controle	+	-	+
Extra investeringen	+	=	-

Voor de doelgroep Rijksoverheid is een Enterprise app store als onderdeel van een EMM/UEM het meest voor de hand liggende distributiekanaal. Indien de doelgroep ook burgers betreft is er maar één oplossing mogelijk, namelijk de publieke app store. Wanneer een dienstverlener meerdere EMM/UEM -systemen heeft (bijvoorbeeld vanwege beveiliginsaspecten) is het het overwegen waard om te investeren in een autonome app store. Het aanbieden van een bedrijfsspecifieke app via meerdere enterprise EMM/UEM app stores is beheermatig niet optimaal. Een centraal distributiekanaal is dan beter. Dit geldt ook voor mobiele diensten die Rijksbreed aangeboden gaan worden vanuit de Rijkscloud. Een centraal distributiekanaal is dan essentieel.

9.7 Beheer van devices en apps

De controle over mobiele devices is beperkt en niet te vergelijken met het beheer van de traditionele werkplek.

Afhankelijkheid OS-updates. Bij mobiele platformen ontbreekt de controle over het tijdstip dat updates van het onderliggende operating system vanuit de leverancier beschikbaar gemaakt worden. Apple Dep biedt momenteel dede mogelijkheid om updates van het operating system uit te stellen of te pushen. Samsung Knox enrollment kan tegenwoordig ook updates pushen. Apple publiceert de updates zonder aankondiging, maar wel met een regelmatige frequentie. Android kent een directe afhankelijkheid van de verschillende device leveranciers waardoor de nieuwste versies van Android niet op alle hardware beschikbaar komt. Het effect is dat er meerdere versies van het operating system aanwezig zijn binnen de installed base. Het advies is om door middel van het instellen van compliancy rules gebruikers te dwingen om de laatst beschikbare versie voor het device te installeren of een minimum versie in te stellen. Zorg verder dat lifecyclemanagement goed is geregeld.

Monitoring. Een actueel beeld van gebruik/user metrics, foutcontrole, performance en feedback is van belang voor goed app-management. Het brengt de volwassenheid van de app in kaart en vormt de verdere doorontwikkeling van de functionaliteit. Aan de platformkant kan gebruik gemaakt worden van tooling als HockeyApp, TestFlight, Crashlytics. Voor het opdoen van gebruikerservaring kan juist gebruik gemaakt worden van “inApp” feedback opties of de review mogelijkheden die de app store zelf levert. Bescherming van persoonsgegevens moet wel goed ingeregeld worden.

Eigenaarschap app. Apps kennen vaak vele wijzigingen in functionele eisen en wensen van de opdrachtgever. Met daarbij de vele updates van de leveranciers op operating system niveau is het van belang snel en adequaat op veranderingen te kunnen reageren. Belangrijk hierbij is om de kwaliteit te handhaven. Dit betekent dat het onderhouden van de app een belangrijk proces is. Als dienstverlener is het belangrijk om goede afspraken te maken met de ap- eigenaar. Deze is immers als opdrachtgever in de lead om op tijd een nieuwe versie te initiëren. Functioneel beheer en lifecyclemanagement dient ingericht te zijn. Als de app niet in eigen beheer is, is goede afstemming met de derde partij van levensbelang om de dienstverlening te kunnen garanderen. Zeker nu steeds meer primaire processen mobiel aangeboden worden.

Back-up. Naarmate telefoons en andere mobiele apparaten toenemen, neemt ook de hoeveelheid gegevens die mensen opslaan (apps) op hun mobiele apparaten toe. Het wordt steeds belangrijker om een goede mobiele back-up strategie te hebben. De volgende mogelijkheden zijn beschikbaar:

- Rechtstreeks van het apparaat naar de Apple iCloud of Google sync.
- Rechtstreeks naar uw computer met iTunes ofvia software van de leverancier van Android devices.
- Een hybride aanpak van beide opties

Het is belangrijk te onderkenen dat niet in alle gevallen de eigenaar van de data invloed heeft op de back-up methode. Neem dit mee in het back-up advies aan de gebuikers van de app.

10. Betrokken Partijen

Bij de totstandkoming van dit document zijn de volgende partijen betrokken.

Namen	Contact	Rol bij app ontwikkeling	Expertise & Verdere bijz.
Algemene Zaken		Beheer Rijkshuisstijl	Rijkshuisstijl
Belastingdienst Leendert Versluijs (schrijver)	l.versluijs@belastingdienst.nl	Ontwikkelt voor burgers, bedrijven & rijksambtenaren native apps. Contactpersoon Referentiearchitectuur Belastingdienst	App architectuur, Ontwikkel proces, Security, User Interface Design, Xamarin, MobileIron
DICTU Ronald Heukers (schrijver)	w.j.r.heukers@dictu.nl	Ontwikkelt voor burgers, bedrijven & rijksambtenaren native apps. Contactpersoon Referentiearchitectuur DICTU	App architectuur, security, MobiDM, XenMobile
DUO		Ontwikkelt voor burgers web apps.	HTML5, Javascript
Forum Standaardisatie		Ontwikkelt digitale standaarden voor de overheid.	Standaarden
Min. van Defensie		Ontwikkelt voor burgers & Defensieambtenaren hybride apps en web apps.	HTML5, Javascript, Apache Cordova, UX Design, MobileIron

Logius		Opdrachtgever voor ontwikkeling authenticatie diensten voor apps.	DigiD, E-herkenning
P-Direkt		Opdrachtgever voor apps in het HRM domein voor rijksambtenaren.	HTML5, Javascript, SAP
Rijkswaterstaat		Opdrachtgever apps voor burgers, bedrijven en rijksambtenaren.	
SSC-ICT Marco Knorren (schrijver)	marco.knorren@minbzk.nl	Ontwikkelt voor rijksambtenaren cross platform native apps.	RijksAppStore (RAS), Xamarin, Blackberry, Appdome
SSC-I Margreet van der Krans Dennis Brocker (schrijvers)	Ssc-i@dji.minjus.nl	Ontwikkelt voor rijksambtenaren en justitiabelen hybride & native apps.	User Interface Design, beveiliging, Blackberry, Mobile Iron
SZW			
VWS			
Politie			
BZK DGOO			
ICTU			
Centrum voor Informatie beveiliging en Privacy(CIP)		expertisecentrum informatiebev. en privacybescherming overheid	Beveiliging, privacy

11. Indicatie kengetallen

Bij de opdrachtverstrekking voor dit document vanuit de CTO-Raad Rijk is een vraag gesteld naar kengetallen met betrekking tot de kosten van het bouwen van een app. Deze vraag wordt hier beantwoord door het aangeven van anonieme ervarings cijfers vanuit twee app ontwikkel organisaties waar de schrijvers deel van uitmaken.

Organisatie 1

De ontwikkelkosten van een app variëren van 50K voor kleine apps tot 1M voor grote apps.

Naarmate UX, Security en Test automation belangrijk is, zijn de kosten hoger.

Onderhoudskosten per jaar bedragen 20% van de initiële kosten. Hieronder wordt verstaan het technisch up-to-date houden en functionaliteit toevoegen op basis van de vraag van gebruikers. Hieronder verstaan we niet de back end kosten.

Organisatie 2

De ontwikkelkosten van een app varieren van 15-25K voor kleine “promo apps” met als doel om content te delen met het publiek, tot 25-100K voor grote maatwerk-apps met content uit de back end en met mutatiemogelijkheden voor gebruiker. Het verschil zit voornamelijk in de keuze voor authenticatie en eventuele notificaties. De kosten voor maatwerk apps met interactie tussen back end systemen (dataverkeer/mutaties) bedragen tussen 50 en 500K. Dit is erg afhankelijk van de complexiteit van de back end.

De verhouding tussen de verschillende ontwikkelactiviteiten zijn:

Ontwikkelactiviteit	Kostenverdeling Organisatie1	Kostenverdeling Organisatie2
Design/Prototyping	20%	10%
PSA en Technisch ontwerp	5%	10%
Bouw	45%	60%
Test	20%	10%
Coordinatie	10%	10%

12. Poster

Deze “poster” is als aparte bijlage beschikbaar.